Crime organisé et crime technologique
Enquêtes et renseignements aux frontières du renouveau

Rapport technique -
Série technologies de l'information

par

Marcel-Eugène LeBeuf, Ph.D.
Mlebeuf@rcmp-grc.gc.ca

École des sciences policières
Collège canadien de police

Ottawa, 2001

105-02797/

This document is also available in English:
www.cpc.gc.ca

Table des matières

Résumé i

Remerciements xi

Introduction générale 1

1- Des développements actuels dans le domaine des technologies et leur impact sur la police 2

2- Les pratiques et méthodes d'enquêtes et d'analyse de la criminalité 9
2.1- Les pratiques d'enquêtes de la criminalité 11
2.2- Les méthodes d'enquête 15
2.2.1- Les unités mixtes d'intervention contre les crimes 20

3- Le renseignement et ses usages 23
3.1- Les buts de la collecte des informations policières 24
3.2- La qualité et l'usage des informations 26
3.3- Le partage des informations- mythe ou réalité 27
3.3.1 Les facteurs de non partage 29
3.3.2 Les conditions de partage 34
3.4- L'alimentation des banques de données - ce qui cause problème 37

4- La nécessité d'une formation adéquate 40
4.1- Des conditions essentielles de succès à créer 43

Conclusion 47

Références 50

Résumé

Introduction

Dans ce rapport deux grandes questions importantes sont explorées, à savoir, le renseignement criminel et les pratiques d'enquête dans un contexte de changement insufflé par l'arrivée des technologies de l'information et par la nécessité reconnue de partager le renseignement criminel. Par rapport aux renseignements criminels, nous évaluons, à la lumière des outils technologiques disponibles, dont les banques de données, les préoccupations des enquêteurs quant à la collecte, l'alimentation et les interrogations des banques. Nous évaluons également l'importance accordée au partage des données colligées. Par rapport aux pratiques d'enquête, il s'agit de savoir jusqu'où la segmentation traditionnelle entre les diverses unités sert réellement la conduite réussie d'une enquête, et plus globalement, le partage réussi des renseignements accumulés à cet effet.

Nous avons rencontré des enquêteurs, des patrons d'unités d'enquête, des directeurs adjoints de plusieurs services de police au pays. Nous avons sélectionné des équipes de travail mixtes où plusieurs services de police collaborent sur une même enquête, comme sur les motards criminalisés par exemple, mais également des unités d'enquête plus traditionnelles comme les unités sur les stupéfiants, les homicides, les crimes économiques, etc.

L'évolution et la pénétration des technologies de l'information dans les organisations, le gouvernement et la société sont rapides. Les technologies créent un espace particulièrement fertile pour des innovations. Elles engendrent aussi une nouvelle culture du travail.

Au Canada, une initiative à au moins deux volets du gouvernement fédéral mérite une attention particulière : le gouvernement en ligne. Le premier volet vise à favoriser les transactions électroniques de tous les ministères du gouvernement avec les citoyens et à mettre en place des dispositifs législatifs pour permettre le commerce électronique sur une grande échelle. Le second volet vise à renforcer la confiance des utilisateurs, à améliorer l'infrastructure d'information sur le commerce électronique et à optimiser les avantages.

Par ailleurs, l'environnement criminel est aussi en train de changer. Internet possède un potentiel de croissance phénoménal. Ce potentiel d'utilisation à des fins légales engendre à son tour un potentiel d'utilisation à des fins illégales.

Dans un contexte où une des priorités du gouvernement fédéral et des provinces est de combattre le crime organisé, il apparaît que deux grandes problématiques se rencontrent : celle de la production de renseignements et d'information pour arriver à développer des stratégies efficaces, et aussi la

compréhension et l'appréhension des outils technologiques utilisés par les citoyens, par les milieux criminalisés et par la police.

La question est donc: comment approcher l'enquête où les technologies de l'information font partie désormais de l'environnement du crime? La question gagne à être posée également à la lumière des grands changements que connaît actuellement le Canada par rapport au crime organisé et aussi en tenant compte des milieux de pratique des enquêtes.

Les pratiques et méthodes d'enquêtes et d'analyses de la criminalité

Dans le domaine des enquêtes, mais pas exclusivement, les habitudes de travail et les manières apprises pour fonctionner perdurent. La formation de base, la formation continue alliées à l'apprentissage sur le tas font qu'il n'est pas facile de "lâcher les vieilles habitudes". C'est dans un contexte en bouleversement et aussi en évolution que les policiers et les enquêteurs font un usage non systématique des outils technologiques mis à leur disposition.

Les pratiques d'enquêtes de la criminalité

Par rapport aux pratiques d'enquêtes et d'analyses, les technologies de l'information restent à ce moment-ci des outils de travail vus encore comme étant relativement nouveaux et menaçants.

Il en découle toutes sortes de conséquences à divers niveaux. Une première importante et déterminante est qu'avant de se demander comment les policiers, les enquêteurs et les analystes utilisent les technologies mises à leur disposition, il aurait fallu préparer l'environnement policier aux grands bouleversements provoqués par les technologies. Une seconde conséquence est directement liée à l'usage ou à l'utilisation réelle ou souhaitable qui est faite. Il découle que l'accès direct engendre des pratiques où le recours à l'ordinateur, et par là aux banques de données informatisées, devient systématique selon la section à laquelle on appartient.

Le développement du personnel et d'une expertise appropriée pour certains, dont les enquêteurs, fait désormais partie de l'évolution de la police. L'expertise est d'autant plus nécessaire que des policiers ne sont pas prêts à enquêter les crimes technologiques parce qu'ils ignorent l'usage des technologies comme l'accès à Internet par exemple, ou encore qu'ils sont incapables d'en évaluer la portée.

Le développement de l'expertise de pointe entraîne à son tour des difficultés majeures pour la police. Les processus de promotion fonctionnent de telle sorte qu'un individu même hautement formé doit quitter son champ de compétence pour accéder à une promotion. Lorsque l'individu quitte sa fonction, il en découle une perte de l'expertise.

Une des conséquences inattendues de l'arrivée et de l'usage des technologies se reflète dans la somme de travail demandée. Les étapes relatives à la collecte des informations et à leur mise en banque apparaissent comme un supplément dans la tâche.

Il est faux de prétendre que les technologies seraient reliées à une question d'âge chronologique ou d'années de services. C'est surtout une question d'attitudes à développer. Par ailleurs, il est normal qu'il existe une période de flottement dans l'apprentissage individuel ou par programme de formation et dans l'aide à donner aux collègues. Enfin, des services spécialisés sont de plus en plus développés pour aider les policiers dans les fonctions reliées à la saisie de disques durs d'ordinateurs par exemple.

Les pratiques d'enquêtes sont influencées par l'accès direct aux outils technologiques comme l'ordinateur, par les possibilités encore peu utilisées de se servir du potentiel des outils comme le CD-ROM. Il faut non seulement continuer d'éveiller la curiosité des individus mais aussi favoriser leur épanouissement.

Les méthodes d'enquête

Nous nous sommes intéressés à la segmentation traditionnelle qui existe dans les enquêtes par la création des différentes unités . Ces unités, comme les unités de crime économique, de crime contre la personne, des stupéfiants, etc., ne favorisent par les contacts entre les policiers soit par tradition ou par apprentissage à la culture.

Il existe un cloisonnement réel et nécessaire entre les unités d'enquête. Ce cloisonnement est le résultat d'une expertise de pointe développée pour rencontrer les difficultés particulières des enquêtes. Le cloisonnement engendre une compétition observable entre les unités, certaines ayant un impact public très grand. Le cloisonnement favorise aussi une expertise de pointe dans un secteur donné.

Les analystes sont une catégorie d'experts dans le domaine des enquêtes, dont les enquêteurs ont besoin. Ils contribuent tout particulièrement au plan de la gestion des informations complexes, au plan de l'orientation d'une enquête et aussi au niveau de la compréhension des divers éléments reliés à l'enquête.

Enfin, il existe une hiérarchie formelle entre les unités d'enquête. Cela entraîne des conséquences sur la publicité accordée, les budgets importants obtenus, les outils comme les téléphones cellulaires, ordinateurs, pagettes, etc., accordés à tous les membres de ces unités.

Les unités mixtes d'intervention contre les crimes

Les unités mixtes rassemblent des policiers de divers services de police et aussi, selon le cas, des agents

d'application de la loi rattachés à divers ministères. L'objectif consiste à rassembler les forces communes pour combattre le crime organisé, par exemple.

Les unités mixtes ne sont pas nouvelles, elles sont en expansion. L'unification des efforts facilite une meilleure coordination des moyens d'action disponibles, des moyens d'enquête et des budgets. Il est considéré que les unités mixtes s'avèrent dorénavant la façon de faire de la police du XXI ième siècle grâce aux alliances ponctuelles. Enfin, les unités mixtes proposent des moyens d'intervention qui permettent de donner un coup de main à des unités ou à des services qui n'ont pas le temps ou qui ne sont pas équipés pour le faire.

Par ailleurs, au moins deux problèmes contreviennent au succès des unités mixtes. Le premier porte sur les habiletés et les compétences des individus en présence qui ne sont pas tous au même niveau. Le second concerne la gestion des unités où les individus prêtés ne se rapportent pas au chef d'équipe pour leur évaluation annuelle, leurs congés, etc. Par contre, un élément positif majeur concerne le partage des informations qui s'en trouve facilité.

Le renseignement et ses usages

Les informations contenues dans les banques de données informatisées ou les dossiers constituent des outils de travail pour les enquêtes en particulier. Un renseignement d'appoint oriente vers les cibles les plus favorables pour des opérations policières efficaces.

Les buts de la collecte des informations policières

Les buts ont été rassemblés en trois catégories. Dans la première, les informations servent de guide pour orienter une enquête ou pour orienter les policiers. Dans la seconde, les informations servent à améliorer la qualité des opérations et à permettre des analyses poussées. Dans la troisième finalement, les informations servent spécifiquement à préparer des affidavits. Il est sous-entendu que les informations sont contemporaines et de qualité.

La qualité et l'usage des informations

Il est important que les enquêteurs aient accès aux informations et aussi qu'ils soient capables de les interpréter convenablement

Une préoccupation quant aux informations est d'encourager la collecte plus globale des informations.

L'exercice porte moins sur le fait de collecter des informations que sur celui de collecter des informations de qualité. Des informations de qualité conduisent à des actions ponctuelles au plan des arrestations et des condamnations. Le manque de coordination entre les différents systèmes et incidemment entre les services de police contribuent beaucoup à une qualité déficiente au plan des informations à recueillir. Enfin, il apparaît que les informations sont utilisées à des fins secondaires, telle que de la vantardise de la part de services de police, puis le partage par la suite.

Le partage des informations - mythe ou réalité

Le partage des informations est en soi une problématique fondamentale pour la police. Elle fait appel aux politiques de coopération entre membres d'un service de police mais également entre les services de police du pays et de l'étranger.

D'emblée, toutes les personnes rencontrées sont d'accord, chacune à leur façon, pour dire qu'en principe, le partage des informations est important. Le partage est soumis à une série de facteurs formels et informels pour protéger les informations, les enquêteurs, les sources ou encore l'enquête comme telle. Selon le contexte et l'enquête, il peut arriver que les renseignements ne soient pas partagés à l'intérieur d'une équipe d'enquête. On peut comprendre alors que les informations ne sont pas rendues disponibles aux membres du service de police, à d'autres services de police au pays et à l'étranger. Le temps nécessaire et les divers systèmes jouent contre les individus.

Les facteurs de non partage

Aux moins quatre familles de facteurs ont été identifiées.

La première est relative à la confiance mutuelle créée et bâtie entre les individus et entre les organisations, et soutenue par tous les niveaux des organisations. En l'absence de confiance les individus sont en général hésitants à donner quoi que ce soit. Une deuxième famille de facteurs repose sur l'aspect légal. C'est la règle de la tierce partie qui s'impose et qui implique que les sources comme les renseignements, ne peuvent être dévoilés si la troisième source des informations refuse. Il y a également les législations sur la vie privée ou sur l'accès à l'information qui limitent ou plutôt circonscrivent les règles du partage et de la protection des renseignements. Enfin, le partage des informations avec les agences internationales se pose également. Une troisième famille relève des méthodes de travail dans le domaine des enquêtes qui sont reliées aux attitudes des individus, aux méthodes apprises par des formations sur le tas avec les collègues et aussi à l'ignorance de la manipulation des systèmes informatisés. Une quatrième famille est constituée par les conditions de travail comme les limites physiques pour consigner les informations.

Les membres d'un service ont accès à des banques de données selon divers niveaux de sécurité. Les systèmes d'entreposage et les outils technologiques ne favorisent pas toujours le partage des informations. Le temps nécessaire et les divers systèmes jouent contre les individus.

Les conditions de partage

Différentes conditions de partage touchent à une philosophie personnelle des individus ou à des obligations structurelles. Dans le premier cas, on explique que dans le contexte des unités mixtes il est impensable qu'une partie des informations ne soit pas dévoilée aux collègues des autres services de l'unité. L'alimentation est aussi favorisée. Une autre condition est liée au moment de la divulgation de la preuve. A ce moment-là, il n'est plus question de cacher les informations qui sont au dossier puisqu'elles seront connues nécessairement des avocats et du tribunal. Enfin, une dernière condition facilitant le partage est liée, dit-on, au manque de ressources pour mener les enquêtes efficacement.

Les informations et le renseignement prennent une valeur différente selon le type d'enquête qui le compose. Or, une faiblesse remarquable au plan des enquêtes est la fermeture traditionnelle des unités d'enquête. Les méthodes de la police feront que les interventions seront ponctuelles et selon la définition qui sera donnée du crime. La cueillette, l'entreposage et le partage des informations restent encore totalement restreints au contexte des unités. A l'intérieur des unités il existe des frictions quant au partage des informations entre les membres de services différents. A l'extérieur des unités, il existe un mur du silence et du non partage total des renseignements.

Les conditions ne favorisant pas ou peu le partage des informations, constituent les deux facettes du même problème. L'une et l'autre apportent des éléments de compréhension et aussi de solutions. A l'heure actuelle, des informations sont échangées si ce n'est que par le biais des grandes banques de données de renseignements comme le Centre d'information de la police canadienne, par exemple. Cela constitue certainement une entreprise importante pour l'application de la loi. Toutefois, dans le cadre d'une enquête de pointe ou moins spécialisée, le renseignement constitue non seulement un outil d'orientation mais aussi la source de départ de l'enquête comme telle.

L'alimentation des banques de données ce qui cause problème

Le partage de renseignements implique nécessairement qu'il y aura eu précédemment une période de cueillette. Cela implique aussi que les renseignements possèdent une valeur par rapport aux besoins de l'enquête ou des enquêteurs impliqués ou encore des stratégies de combat.

Un des principes de la bonne alimentation des données est que si le renseignement ne sert pas dans un dossier, il est mis dans la banque pour servir à quelqu'un d'autre. Les pratiques actuelles des enquêteurs les amènent à focaliser sur les informations très pointues relatives à une enquête. Les informations qualifiées de secondaires sont laissées de côté.

Les pratiques d'alimentation sont affectées par au moins quatre facteurs. Le premier porte sur le comment faire ou sur les apprentissages d'une méthodologie de travail. La charge de travail imposée aux enquêteurs devient un argument justifiant une alimentation partielle ou encore une non alimentation. Le second facteur s'illustre par les sources d'information : que va-t-on cueillir? De façon générale, disons que la majorité des enquêteurs rencontrés s'entendraient pour dire que l'information recueillie doit être contemporaine et actuelle parce qu'elle est directement utile dans le cours d'une enquête. La cueillette et les efforts pour s'assurer de la pertinence du matériel sont vus comme exigeants et astreignants. Plusieurs enquêteurs voient le renseignement comme étant directement utile dans l'enquête au point où il pourra être utilisé en preuve au tribunal ou qu'il permettra de procéder à des arrestations et à des condamnations. Un troisième facteur porte sur les sources d'information. Il s'agit de voir encore ici s'il existe une dynamique pour tirer le maximum des sources possibles. Un quatrième facteur est l'apport de la technologie. Il apparaît que les outils technologiques nécessaires ne sont pas mis à la disposition des gens et qu'il y a aussi un manque de ressources humaines pour entrer les données dans les banques.

La nécessité d'une formation adéquate

La nécessité d'une formation adéquate est nettement reconnue par les interviewés et par beaucoup d'intervenants dans le domaine de la police. Certains diront que la formation se doit d'être spécialisée de sorte que les policiers puissent suivre rapidement l'évolution de leur domaine d'enquête. Il faut qu'elle soit offerte et donnée au moment opportun, ce qui ne semble pas être le cas pour la grande majorité des individus interviewés. Enfin, une des grandes difficultés de la formation dans le domaine des enquêtes est le roulement du personnel.

Il arrive que l'apprentissage aux fonctions soit fait directement sur le terrain et avec le temps.

Un certain nombre d'interviewés ont été en mesure d'évaluer les conséquences résultant d'une absence de formation adéquate ou d'une formation partielle dite sur le tas auprès des collègues. Les personnes peu ou pas formées doivent nécessairement s'appuyer sur les collègues pour obtenir informations et conseils. Cela veut dire une perte de temps appréciable autant pour les nouveaux venus que pour les policiers d'expérience. La nécessité de se fier constamment aux collègues, du moins pour un temps indéfini, signifie potentiellement des erreurs ou l'absence d'action. Il peut aussi y avoir des conséquences plus dramatiques où des erreurs judiciaires entraînent la perte de causes qui ont engendré des coûts élevés.

On a demandé aux individus s'il y avait des thèmes ou des questions plus spécifiques qui devraient être traités lors des programmes de formation. Il apparaît important de développer des programmes de formation et d'offrir davantage une formation de pointe et à la carte pour répondre aux besoins spécifiques d'une clientèle type.

La formation concerne aussi et surtout le développement des législations et de la jurisprudence. L'une comme l'autre exercent une influence sur les pratiques et sur les méthodes de travail.

La formation dans le domaine des enquêtes, entre autres celles sur le crime organisé et la cyber-criminalité, n'a pas été donnée systématiquement aux policiers interviewés, quel que soit le service de police auquel ils appartiennent. Les programmes de formation portant sur les niveaux d'enquête, débutant et avancé, sont vus comme pertinents de la part de ceux qui les ont suivi, très peu de personnes interviewées. Par contre, il se dégage un consensus sur la nécessité de tenir les enquêteurs au courant de l'évolution des législations, de la jurisprudence et des habiletés développées.

Il fut aussi mentionné qu'on sabre trop souvent dans les budgets. À long terme, les pratiques policières en souffrent lorsque sont commises des bavures, des erreurs judiciaires ou que les façons d'enquêter sont tout simplement inadéquates.

Des conditions essentielles de succès à créer

On peut identifier plusieurs facteurs qui peuvent être déterminants dans la bonne marche d'une enquête. Il faut du personnel en nombre suffisant, des budgets adéquats, une formation donnée et adaptée, l'usage d'outils technologiques de pointe, etc. Un programme de formation n'exerce aucune influence sur la plupart de ces facteurs. Il peut potentiellement jouer, par contre, sur les attitudes et sur les mentalités. Il peut par ailleurs améliorer les compétences des individus.

Le vrai défi pour l'enquêteur, et ajoutons ici l'analyste, est de dépouiller les faits en faisant appel à la fois au bon jugement, à l'intuition et à la déduction. Ces aspects deviennent d'autant plus importants que les technologies de l'information ont engendré de nouvelles façons de communiquer, un langage, des façons de faire ainsi que leur propre épiphénomène nommé *hacker, cracker, phreaker*. Les programmes de formation offerts aux policiers mettent probablement trop de côté les qualités à développer parce que cela implique un investissement personnel important, à plus ou moins long terme et qui prend certaine distance par rapport aux techniques magiques enseignées. Ces qualités semblent se situer en conjonction directe avec la culture des technologies de l'information. Ce n'est pas seulement le langage des ordinateurs qu'il faut posséder mais aussi la compréhension du nouvel environnement qu'il crée.

Dans un univers en développement aussi rapide, les futurs enquêteurs devraient avoir les compétences suivantes : expérience, compétence, bonne capacité d'analyse, souplesse pour adapter son milieu de travail à l'évolution des technologies, aux législations à venir et à leur application. Il serait aussi souhaitable que les individus puissent créer un système de réseau avec l'entreprise privée des technologies.

La formation devrait porter non seulement sur les techniques mais également sur des exercices de

logique, de déduction et d'évaluation des cas difficiles. Des exercices sous forme de scénarios devraient favoriser l'in-put des étudiants, leur capacité de compréhension et de développement et leur faculté de déduction.

Par ailleurs, d'autres pistes demandent à être explorées. Elles concernent les entreprises de collaboration entre la police et divers groupes intéressés par la sécurité. Elles portent aussi sur les alliances entre les différentes agences gouvernementales et aussi entre les pays. Mais comment parvenir à les actualiser? Chaque organisation est soumise à des normes légales, à des champs de pratique et à des règles éthiques. Quels sont les enjeux en présence, quelles sont les possibilités de partage des informations possédées par les unes et les autres, quels sont les outils disponibles pour le faire, quelles sont les limites au partage des renseignements personnels possédées à la lumière des lois sur la vie privée, quelles sont les embûches techniques à surmonter? Voilà les points majeurs à évaluer afin de parvenir à créer des partenariats dans le combat contre le crime.

On peut imaginer qu'une mise en commun des outils, des méthodes de travail et des intérêts communs pourrait se faire lors de séminaires de formation pointue et adaptée à la réalité des organisations en présence.

Le partenariat s'illustre aussi par le biais d'une certaine forme de coordination entre les agences d'application de la loi. On peut imaginer le développement d'une banque de données qui porterait par exemple sur les formes sophistiquées de crimes technologiques, sur les modèles d'action, afin de développer par la suite des programmes de prévention. On peut aussi entrevoir le développement d'une liste d'acteurs ou d'unités dans le domaine d'application de la loi qui se penchent particulièrement sur le crime organisé et sur le cybercrime. Des enquêtes faites par des firmes spécialisées sur l'état de la pénétration des systèmes informatiques pourraient être d'une grande utilité pour les processus de prise de décision dans la police.

Conclusion

Les limites actuelles dans le domaine des enquêtes se résument comme suit. Il y a un personnel insuffisant et en continuel mouvement. Il arrive que des individus de l'unité des homicides soient prêtés à une autre unité, ou encore que les équipes qui se penchent sur le crime informatique soient petites. Il arrive aussi très régulièrement que les individus quittent une unité d'enquêtes pour obtenir une promotion. Ils quittent alors avec une expertise pour en développer une autre ailleurs.

Par ailleurs, les budgets disponibles sont trop souvent limités, ou encore les budgets actuels ne permettent pas d'avoir accès aux outils nécessaires pour mener des enquêtes efficaces.

En ce qui concerne la formation des enquêteurs, on pourrait dire qu'elle n'est pas toujours adaptée au contexte, qu'elle n'est pas offerte au bon moment, ou encore qu'elle n'a jamais été reçue, et enfin,

qu'elle n'est pas perçue comme étant essentielle.

Il ressort que par rapport aux crimes reliés aux technologies de l'information, il faut développer une expertise d'enquête au plan de la compréhension des façons de faire plutôt que d'essayer de devenir un expert en informatique ou en gestion de systèmes. Il existe une grande catégorie d'experts dans le domaine des technologies. Il reste aux policiers à apprendre à travailler avec ceux-ci.

En ce qui touche le cybercrime, le terrorisme informatique et les nouvelles formes de crime reliées à l'environnement, on peut dire sans s'y méprendre qu'il y a à ce jour une méconnaissance réelle des problématiques et des enjeux. Plus souvent qu'autrement, les interviewés on vu ces questions comme relevant d'unités spécialisées ou encore d'agences autres que la police. En ce sens, on peut dire que la police prépare peu ses policiers à l'évolution de la société.

Enfin, il existe définitivement une culture des enquêtes. Cette culture maintient les individus dans des boîtes, que certains nomment silos. Elle contrevient à leur façon à la collaboration entre collègues, au partage des informations et finalement au succès des enquêtes. Une piste de solution serait de former les enquêteurs dans des programmes de formation conjoints sur la collaboration et le partage mais aussi sur la capacité d'aller chercher l'expertise là où elle se trouve. Encore maintenant, le partage se fait d'une façon unilatérale de la part entre la police et les agences et entre les services de police de grande taille avec ceux de moindre taille, et avec les grandes corporations qui collaborent avec la police. À moyen terme et à long terme, ceci devient contre-productif. Il reste donc à développer une culture du renseignement qui ne soit pas limitative.

Une approche proposée consiste à focaliser sur les types de partenariat à créer avec les autres agences d'application de loi dans l'esprit des meilleures pratiques et des grandes leçons retenues; il s'agirait également de focaliser sur le type de partenariat à développer avec la police privée, les agences de sécurité des grandes corporations comme les banques par exemple; enfin il faudrait également focaliser sur un partenariat à développer avec la grande industrie reliée aux technologies de l'information. Ces dernières assument la responsabilité de développer des outils pour la société et il appartient à la police de développer des moyens pour utiliser ces outils.

Remerciements

L'auteur voudrait remercier chaleureusement les nombreuses personnes qui ont accepté de partager leurs opinions, valeurs et connaissances de leur milieu de pratique reliés aux enquêtes. Sans eux, ce rapport n'aurait pas la qualité qu'il possède.

Introduction générale

Dans le cadre d'un programme de recherche portant sur les technologies de l'information dans la police au Canada, nous avons exploré diverses avenues relatives à l'arrivée et à l'implantation des technologies modernes dans la police (LeBeuf, 2000a). On a constaté que la police a, depuis longtemps, commencé à intégrer des technologies pour améliorer l'efficacité de la mise en application de la police, telles les banques de données comme le Centre d'information de la police canadienne par exemple, et beaucoup d'autres (Soullière, 1999). On a également remarqué que la police est présentement confrontée à un certain nombre de transformations majeures relatives à l'intégration des outils technologiques, à la poussée phénoménale engendrée par la globalisation des systèmes, et enfin, aux contraintes liées à la standardisation des outils, des techniques et des méthodes de travail en général (LeBeuf, 2000b). Ces transformations constituent une poussée irrémédiable et irréversible vers un changement de paradigme de la police publique. On a également constaté qu'à l'heure actuelle, il convient de partager les informations avec des outils convenables et compatibles. Il convient également de s'engager dans des exercices sérieux de planification de budgets récurrents et de programmes de formation à actualiser. Enfin, nous avons constaté que la police avait en général une méconnaissance des outils, du marché et des pratiques reliés aux technologies. La police doit s'adapter aux technologies et au rythme imposé par le marché. Déjà des expériences en Grande-Bretagne montrent que des polices privées et des fournisseurs de services d'Internet jouent un rôle de premier plan dans le contrôle d'activités illégales sur le *net* (Wall, 1998). Or, la police possède un rôle de maintien de l'ordre et dans ce contexte, elle doit prendre les meilleures avenues pour y réussir. Si l'ordre social est en train de changer, comme nous le voyons, il appartient à la police de suivre et de s'intégrer à ce changement.

Dans ce rapport, nous explorons tout particulièrement deux grandes questions importantes, à savoir le renseignement criminel et les pratiques d'enquête dans un contexte de changement insufflé par l'arrivée des technologies de l'information et par la nécessité reconnue de partager le renseignement criminel. Par rapport aux renseignements criminels, nous évaluons, à la lumière des outils technologiques disponibles dont les banques de données, les préoccupations des enquêteurs quant à la collecte, l'alimentation et les interrogations des banques. Nous évaluons également l'importance accordée au partage des données

colligées. Par rapport aux pratiques d'enquête, il s'agit de savoir jusqu'où la segmentation traditionnelle entre les diverses unités sert réellement la conduite réussie d'une enquête et plus globalement le partage réussi des renseignements accumulés à cet effet. Il restera à évaluer ultérieurement les grandes leçons des méthodes de travail dans le domaine de la sécurité.

Nous avions constaté précédemment que des enquêteurs avaient peu recours à l'usage des technologies dans le cadre de leur travail. Plusieurs facteurs étaient retenus pour expliquer cet état de fait, dont le manque d'accès aux ordinateurs et le manque de formation pour leur usage (LeBeuf, 2000c; LeBeuf et al, 1999).

La grande originalité de cette recherche repose sur le fait qu'elle est en grande partie alimentée directement par les individus qui oeuvrent dans le milieu des enquêtes, tout particulièrement sur le crime organisé mais pas exclusivement, et celui des analystes. Nous avons rencontré des enquêteurs, des patrons d'unités d'enquête, des directeurs adjoints de plusieurs services de police au pays. Nous avons sélectionné des équipes de travail mixtes où plusieurs services de police collaborent sur une même enquête, comme sur les motards criminalisés par exemple, ainsi que des unités d'enquête plus traditionnelles comme les unités sur les stupéfiants, les homicides, les crimes économiques, etc. Or, comme les technologies de l'information sont importées dans la police, il appartient aussi de voir comment les technologies de l'information ont commencé à bouleverser les pratiques sociales des enquêteurs. La prémisse de départ est que les meilleurs informateurs, dans le sens large du terme, sont ceux-là mêmes qui sont confrontés aux technologies de l'information à cause de leur emploi. Ils sont les mieux placés pour traiter de thèmes importants mais peu discutés dans le quotidien animé des opérations policières.

1- Des développements actuels dans le domaine des technologies et leur impact sur la police

Afin de comprendre l'ampleur des transformations auxquelles sont confrontés les services de police au pays, il convient de s'attarder à quelques-unes des transformations qui touchent présentement la société canadienne et le monde.

L'évolution et la pénétration des technologies de l'information dans la société et les organisations, dont les gouvernements, sont rapides. L'évolution est d'autant plus rapide que les personnes sont de plus en plus éduquées et par là elles deviennent plus à même d'évaluer leurs besoins, de comprendre les enjeux reliés aux technologies et de faire des choix plus éclairés. Les technologies créent un espace particulièrement fertile pour des innovations. Denning (1998) en trace une liste d'une quinzaine qui touchent à tous les secteurs dont la propriété intellectuelle, la formation à distance, l'intelligence artificielle, la réalité virtuelle, la téléprésence et d'autres. La téléprésence ouvre la porte au travail à la maison et donc à une fuite des lieux de travail traditionnels. Les technologies engendrent aussi une nouvelle culture du travail (new work culture) (GRC, 2000) caractérisée par une circulation plus large et libre des idées, par l'application de méthodes de travail novatrices comme l'usage répandu du courrier électronique jusqu'à devenir une "e-mail personne"selon l'expression de Field (2000), et par des alliances ponctuelles et provisoires pour des tâches spécifiques. Ces réseaux sont aussi constitués par les groupes criminels. Cette évolution ne doit pas nous faire oublier que les humains sont confrontés à des bouleversements parce que leurs pratiques et leurs habitudes sont modifiées ou appelées à l'être. Les technologies comme le mentionnait Norman (2000) gagneraient à rester invisibles en autant que les humains sont capables de les utiliser comme support et comme réponse directe à leurs besoins.

Au Canada, une initiative à au moins deux volets du gouvernement fédéral mérite une attention particulière. L'initiative vise à favoriser les transactions électroniques de tous les ministères du gouvernement avec les citoyens et à mettre en place des dispositifs législatifs pour permettre le commerce électronique sur une grande échelle. Reprenons-les.

Intitulé le gouvernement en ligne (Government On-Line) sous la responsabilité du ministère de la Justice, un des volets vise à moderniser les services offerts aux citoyens. Ainsi, les services seront offerts plus directement, plus rapidement, 24 heures par jour sur le territoire (voir GRC, 2000: 35 et ss). Le second volet, tout aussi ambitieux, porte sur le commerce électronique sur une grande échelle. Comme souligné ailleurs (Dryden, 1998), le commerce électronique n'est pas nouveau. Des transferts de fonds se font depuis plusieurs années. Mais actuellement, le développement, l'accélération et l'intérêt suscité par les entreprises et les consommateurs donnent une ampleur différente. Située en droite ligne avec les préoccupations de l'organisation de coopération et de développement économique (OCDE), l'initiative vise à renforcer la confiance des utilisateurs et des consommateurs, à établir des règles fondamentales

pour régir le marché numérique, à améliorer l'infrastructure d'information sur le commerce électronique et à en optimiser les avantages (Dryden, 1998). Vu comme supportant l'agenda économique du gouvernement en place, il s'agit de favoriser une augmentation de l'économie digitale et numérique où les transactions se font par des moyens électroniques (Canada, 2000). L'objectif est d'atteindre 5% du commerce électronique mondial en 2003 (GRC, 2000). A cet effet, le gouvernement a adopté la Loi sur la protection des renseignements personnels (C-6) prenant effet en janvier 2001, reconnaissant légalement la signature électronique. En cela, le Canada suit l'exemple des Etats-Unis, de l'Union européenne et de plusieurs pays d'Europe (Murray, Vick, Wortley, 1999).

La pénétration des technologies de l'information crée un champ fertile de nouvelles menaces à la sécurité et aux humains (Lenton, 2000). Par exemple, il a déjà été constaté à quel point les gouvernements sont victimes de leurs employés par le biais des technologies de l'information. On parle ici de fraudes, de mauvais usages des ordinateurs, des attaques sur les systèmes informatiques, de propagande terroriste, de vengeance, etc. (Smith, 1999). On sait aussi que le cybercrime commercial touche à la fois l'application de la loi et du milieu des affaires (Livanos Cattaui, 1999). On peut imaginer qu'avec l'encouragement des gouvernements pour s'engager dans le commerce électronique les gouvernements devront aussi s'engager sérieusement dans la mise sur pied de mécanismes de contrôle adaptés non seulement aux nouveaux moyens mis en place mais aussi aux transformations des mentalités engendrées par les technologies. Car en effet, toute nouvelle forme de commerce amène nécessairement un nouveau type de criminalité (White, L., 2000). On pourrait ajouter aussi qu'elle amène aussi à adapter des mesures existantes. Par exemple, la compagnie d'assurance Lloyds of London, se préparerait à mettre à la disposition des compagnie une police d'assurance en cas de *hacking* (hacking insurance) (White,C., 2000).

La menace d'une destruction des infrastructures technologiques est aussi présente et prise très au sérieux. Un groupe de travail du *Center for Strategic and International Studies* de Washington a évalué les multiples aspects de cette question (CSIS, 1998). La liste des recommandations montre à elle seule le sérieux des enjeux.

L'environnement criminel est aussi en train de changer. Suite à une enquête majeure relative au télémarketing impliquant 951 sujets, le *FBI* a saisi 92 ordinateurs mais seulement trois armes à feu

(Robertson, 1999). Comme l'ont noté Boni et Kovacich (1999), aujourd'hui les crimes commis dans l'environnement contemporain des affaires assurent le succès aux criminels qui opèrent en ayant les connaissances relatives aux technologies et à l'autoroute de l'information. Les outils (pour le faire) sont disponibles. La technologie des *microchips*, la *nanotechnologie* (Drolet, Moen, 2000), la technologie sans fil sont actuellement disponibles et utilisées par le grand public. Ce qui était considéré futuriste il y a à peine quelques années est dorénavant en usage.

Internet, dont le potentiel de croissance est phénoménal, est passé de 19% d'utilisation en janvier 96 dans les foyers et ailleurs au Canada, à 60 p.cent en janvier 2000, ce qui constitue une forte augmentation dans l'usage (Ekos Research Associates, 2000). Ce potentiel d'utilisation à des fins légales engendre à son tour un potentiel d'utilisation à des fins illégales. Le paiement électronique permet des transactions rapides, anonymes et non supervisées étant donné leur très grand nombre (Alexander, Munro, 1996). Un tel système devient vulnérable pour les personnes qui souhaitent blanchir de l'argent. En effet, le *web* assure un certain anonymat entre autres par les techniques d'encryption (FBI, 1999) ou autres logiciels performants (Scientific American, 2000). Il constitue en quelque sorte un tampon limitant et retardant les possibilités de se faire intercepter parce que les preuves ne sont pas tangibles et peuvent être facilement éliminées (Robertson, 1999; Sullivan, 1999). De plus, le temps et l'espace sont annulés. À ce moment-ci, il est encore relativement difficile de connaître la fréquence des crimes. Soit qu'ils ne sont pas dénoncés, soit qu'ils sont peu commis, ou soit que les agences d'application de la loi ne savent pas encore comment recevoir et colliger les plaintes relatives aux crimes commis avec les technologies de l'information. Il semblerait qu'à l'heure actuelle pas plus de 10% des crimes reliés à l'ordinateur seraient rapportés (Davis, Hutchison, 1997). Le crime cybernétique pose un défi unique en ce sens qu'il se situe en périphérie des méthodes traditionnelles d'enquêtes de la police (IACP, 1999).

Plusieurs articles donnent des détails sur l'usage d'Internet pour le blanchiment d'argent (Sambugaro, 2000), sur les performances phénoménales de certains *hackers* comme celui du vol de 300 000 numéros de carte de crédit (Organized Crime Digest, 2000b), ou celui des adolescents de 14 et 16 ans qui ont utilisé des numéros de carte de crédits de plusieurs centaines d'individus (Organized Crime Digest, 2000a), sur l'expansion des opérations bancaires clandestines (underground banking) (Sambugaro, 1999), sur les fraudes électroniques (White, L., 2000). A ce sujet, selon un sondage rapporté par Deloitte, Touche et Tohmatsu, il semblerait que la moitié des plus grandes compagnies au monde ont été

victimes de fraude durant leur dernière année fiscale. De celles-ci , 25% ont rapporté des pertes d'au moins un million de dollars au cours des cinq dernières années (Deloitte Touche Tohmatsu, 1999). Par ailleurs, selon des estimés, il y aurait eu en 1998 une perte de plus de 16 milliards de dollars américains causée par la fraude sophistiquée de faux chèques (Robertson, 1999).

La criminalité cybernétique reste encore difficile à définir. Une des approches du crime cybernétique a été de le définir ainsi: selon la situation, l'ordinateur est soi l'objet du crime ou soit l'instrument du crime (Carter, Katz, 1998). Pour le dire autrement, l'ordinateur est impliqué ou associé au crime. Présentement, dans le champ de l'application de la loi reliée au crime cybernétique, on pourrait résumer les deux positions qui se rencontrent chez les intervenants. Elles se situent en position dichotomique presque exclusive. D'une part, certains diront que le crime par ordinateur n'est en soi rien de neuf. La seule nouveauté est le recours à un nouvel outil performant. Au harcèlement (cyberstalking) par ordinateur, le commentaire devient le suivant: "tu n'attends pas avant de fermer ton ordinateur". En d'autres mots, fermer l'ordinateur éliminerait la source du crime pour la victime, ce qui n'est que partiellement vrai, surtout si la victime doit utiliser son ordinateur pour son travail. D'autre part, certains diront que la criminalité cybernétique prend un autre visage parce qu'elle est causée dans un nouvel environnement. Autant au XVIII ième siècle le vol en Angleterre était peu existant parce que les gens ordinaires possédaient peu de biens, mais ils étaient fortement punis quand il s'agissait de vol de chevreuils (Thompson, 1975), autant de nos jours les gouvernements et les services de police se sont engagés dans la mise sur pied de programme de prévention du vol. L'environnement comme la possession des biens se sont transformés. Ainsi, le harcèlement électronique est moins physique que virtuel ce qui ne veut pas dire que les répercussions pour la victime sont moindres; ou encore, le *hacking* une activité née essentiellement par la dispersion d'ordinateurs à un très grand nombre d'usagers. Le vol des outils comme tel reste aussi un crime. Selon des estimations récentes, les pertes reliées au vol de matériel (hardware) sont évaluées à $34.7 millions de dollars américains pour la période couverte entre octobre 1997 et juin 1998 (Dertouzos et. al., 1999). Les coûts de remplacement sont très élevés.

Parmi les tentatives pour conceptualiser le crime cybernétique un article du TELEMASP Bulletin (2000) est éclairant. Il présente cinq catégories qui ne sont pas mutuellement exclusives mais qui reflètent la poussée de la nouvelle criminalité. Une, l'ordinateur est la cible du crime - par exemple prendre des informations de la mémoire d'un ordinateur, ou encore endommager volontairement un programme ou le

hardware; deux, l'ordinateur est un instrument du crime, par exemple les fraudes relevant de transactions avec un ordinateur, les fraudes en télécommunications. Trois, l'ordinateur est un accessoire pour commettre un autre crime, par exemple le blanchiment d'argent, la distribution de matériel pornographique, etc. Quatre, le crime est associé à la généralisation des ordinateurs, par exemple la violation des droits d'auteurs, le marché noir des mémoires volées d'ordinateurs, l'équipement contrefait. Cinq, le méfait en réseau (networking malfeasance), par exemple le harcèlement, la diffamation d'un individu par des messages électroniques sur un réseau, l'accès non autorisé à un ordinateur "juste pour explorer le système". Une autre approche, celle de Wall (1998), propose une typologie des crimes connus. Les groupes de crimes cybernétiques les plus identifiés sont le *cybertrespass* que nous traduisons par entrée numérique illégale, à défaut d'une terminologie plus pertinente, référant entre autre au piratage électronique, le *cybertheft* ou disons le vol cybernétique incluant entre la fraude, le jeu virtuel, le *cyberobscenity* ou l'obscénité cybernétique qui traite entre autres de la pornographie infantile, et le *cyberviolence* ou la violence cybernétique où on retrouve les crimes haineux, le harcèlement (voir aussi Sheriff, 1999).

Pour Wall (1998), la tendance actuelle est de focaliser davantage sur les crimes que sur les personnes qui les commettent ou sur les victimes. On peut comprendre alors le commentaire d'un des gestionnaires supérieurs que nous avons rencontré : "actuellement il n'y a pas de sentiment que la police se sent dépassée. Je pense que la connaissance de la police de l'Internet est équivalente à la connaissance de la population générale...les messages e-mail, le harcèlement, il y a des moyens de les détecter. On n'a pas des plaintes" (no 16). Pourtant, le courrier électronique entre autre est un outil fortement utilisé. Selon un sondage mené en 1998 auprès de 10 000 utilisateurs d'Internet et du www, 93% des répondants ont considéré que le courrier électronique était l'outil le plus indispensable (Boni et Kovacich, 1999).

Certains se demandent présentement comment faire la police sur le *net*. Mais la vraie question est plutôt : comment enquêter la nouvelle criminalité issue des méthodes relatives aux outils technologiques, mais aussi la criminalité issue d'alliances entre des groupes organisés, de la criminalité où il y a aussi usage des moyens traditionnels, enfin de la criminalité émergente et non encore codifiée, soit celle de la menace à l'environnement. L'un et l'autre des types de criminalité mentionnés peuvent conjuguer plusieurs des caractéristiques énumérées. Ainsi, des membres de différents groupes du crime organisé peuvent s'associer dans une entreprise criminelle de fraude commerciale sur une très grande échelle en ayant

recours au *web* mais aussi à des pratiques plus physiques d'intimidation. Ou encore, on peut imaginer le même type de groupes impliqué dans des pratiques de déversements illégaux de déchets toxiques désastreux pour l'environnement comme cela se pratique déjà (Porteous, 2000). Les personnes ou groupes de personnes impliquées dans les organisations criminelles dans le but de faire des gains économiques ne se limitent plus uniquement aux groupes traditionnels comme la mafia italienne mais incluent aussi d'autres groupes dans des secteurs restreints (Porteous, 1998). Les entreprises criminelles sont impliquées dans la criminalité cybernétique de plusieurs façons et de façon fructueuse selon les coûts estimés à plus de 10 milliards de dollars américains de pertes annuelles (TELEMASP Bulletin, 2000). Le TELEMASP Bulletin (2000) trace une liste explicite et détaillée de dix activités allant du marché noir, au jeu virtuel, à l'immigration illégale, à la fraude en télécommunications, au commerce sexuel et au vol d'identité.

Avec ce type de criminalité de nouvelles mesures de prévention sociale deviennent nécessaires (Nations Unies, 1999; Parsons, 1998) mais aussi de nouvelles approches en sécurité seront aussi à développer de sorte que "le voleur qui utilise ses yeux plutôt qu'une arme", selon l'expression de Blackburn (2000), pour obtenir votre numéro de carte de crédit pourra aussi être évincé. Deux exemples récents d'intervention méritent d'être mentionnés. Au mois de février 2000, plus de 150 organisations de 28 pays, dont des agences fédérales américaines, des *attorney general*, des bureaux de protection des consommateurs, des *Better Business Bureau*, et aussi le *Hong Kong Consumer Council*, la *University of Texas Law School* sous l'égide du *Federal Trade Commissions's Bureau of Consumer Protection* ont patrouillé le *net* afin d'identifier des pratiques commerciales douteuses. Plus de 1600 sites suspects ont été identifiés et informés que des agences d'application de la loi étaient contactées à cet effet (The Report on Crime & Profiteering, 2000). Par ailleurs, le président du *International Marketing Supervision Network*, une organisation réunissant des agences d'application de la loi, mais aussi des agences gouvernementales, des bureaux d'affaires et des individus de 29 pays pour combattre la fraude sur le *net*, a recommandé une mise en commun (et à jour) des lois de protection des consommateurs au plan national et international (Organized Crime Digest, 2000c). On constate que les interventions souhaitées ne se font plus uniquement par le biais des approches traditionnelles des lois criminelles mais aussi par le recours à des lois civiles. On constate également que ces deux exemples sont une démonstration directe de partenariat entre les agences d'application de la loi et d'autres acteurs intéressés et peu invités traditionnellement à travailler avec la police.

La littérature récente regorge de textes sur les grandes questions relatives aux méthodes d'enquêtes pour les crimes commis avec des technologies de l'information comme les ordinateurs (voir entre autres Icove et. al, 1995; Osterburg, Ward, 1997; Mendell, 1998; Richards, 1999). De plus, comme pour montrer l'importance que ce type de crime est en train de prendre présentement, Janet Reno le précédent *Attorney General* des États Unis, a débloqué des fonds substantiels pour comprendre la complexité du phénomène et pour développer des programmes de formation adaptée (USA, 1999; Williams, 1999). Dans un contexte comme le nôtre où une des priorités du gouvernement fédéral et des provinces est de combattre le crime organisé, il apparaît que deux grandes problématiques se rencontrent:

- la production de renseignements et d'information pour arriver à développer des stratégies efficaces
- la compréhension et l'appréhension des outils technologiques utilisés par les citoyens, par les milieux criminalisés et par la police.

Les exemples cités plus haut nous permettent de réaliser que les pratiques d'enquêtes ont commencé à se transformer et vont définitivement connaître des changements profonds. La sélection des enquêteurs et leur formation doivent dès lors être adaptées. La rapidité, la facilité, le semblant de non barrières traditionnelles rappellent à quel point il est facile, par exemple, de frauder une institution dans un pays X par le biais d'un serveur situé dans un pays Y par un individu résidant dans un pays Z. La menace est là.

La question est donc : comment approcher l'enquête où les technologies de l'information font partie désormais de l'environnement du crime? La question gagne à être posée également à la lumière des grands changements que connaît actuellement le Canada par rapport au crime organisé et aussi en tenant compte des milieux de pratique des enquêtes.

2- Les pratiques et méthodes d'enquêtes et d'analyse de la criminalité

Le domaine des enquêtes est reconnu comme étant un univers particulier dans la police. Les policiers travaillent sans porter l'uniforme de service et quelquefois en jeans et t-shirt. Ils ont des horaires de travail variables collés en fait sur les opérations de surveillance et d'interceptions. Ils ont une relative autonomie dans l'approche à développer selon le type de criminalité qu'ils enquêtent. Ils sont aussi soumis à colliger des informations, à analyser le renseignement et à trouver des pistes pour contrer la criminalité.

Dans le domaine des enquêtes, mais pas exclusivement, les habitudes de travail et les manières apprises pour fonctionner perdurent. La formation de base, la formation continue alliées à l'apprentissage sur le tas font en sorte qu'il n'est pas facile de "lâcher les vieilles habitudes " (no 11), comme on le soulignait. Les préoccupations pour des actions plus efficaces contre le crime organisé à partir, entre autres, de la création des unités mixtes mais aussi par un encouragement à recueillir des informations et à les mettre dans des banques de données informatisées prennent moins leur source dans le combat contre le crime organisé que dans un changement culturel à initier afin d'être efficace. Pour le dire autrement, il apparaît moins important de s'engager dans un combat contre le crime organisé que d'unir les forces pour engager ensemble les services de police. Or, même si d'emblée il existe une volonté de le faire, il reste que des irritants culturels persistent. "Le plus gros problème est d'amener les gars à travailler ensemble" (no 18). Il est question ici autant de développer une vision commune, des objectifs communs et de voir comment chacun peut contribuer à atteindre les buts fixés. Il existe aussi des grandes hésitations par rapport à la question de rendre compte des actions (accountability) dans un contexte où il serait normal de prendre des risques calculés. Comme il nous a été souligné: "risk management is more the management part then the risk part" (no 2).

C'est dans un contexte en bouleversement et aussi en évolution que les policiers et les enquêteurs font un usage non systématique des outils technologiques mis à leur disposition. Trois remarques sont essentielles ici.

Premièrement, il apparaît faux de prétendre que les rapports à l'ordinateur seraient une question d'âge, les plus jeunes policiers étant davantage enclins à les utiliser que les plus âgés (autant en terme d'années de service que d'âge réel). "On ne peut pas généraliser. Des jeunes ont peur, des 25 ans d'expérience en raffolent" (no 5). On encore: "quand on prend des policiers d'expérience qui s'intéressent à l'informatique ils sont une coche au-dessus. Notre doyen avec 32 ans de police a découvert l'informatique sur le tard et il était une bête de performance. Tout l'intéressait. Il nous a formés. Il a développé l'informatique au cours des quatre à cinq dernières années de sa carrière" (no 19).

La seconde remarque porte sur la période de flottement relative à l'acclimatation et à l'usage des technologies. Il est normal d'avoir un certain nombre de difficultés quand vient le moment de faire usage d'un nouveau logiciel ou d'un nouvel ordinateur, d'une banque de données mise à niveau (upgraded).

Une telle période, qui peut être longue, est décrite comme une perte de temps inconsidérée (no 12) quelle que soit la position dans l'organisation. L'apprentissage individuel ou par programme de formation formel, le support, l'aide aux collègues, mais également l'usage du clavier pour entrer les données dans des ordinateurs, sont aussi considérés comme une perte de temps. Ainsi les commentaires suivants: "la technologie nous retourne en arrière. On perd notre temps à nous demander à pitonner" (no 15, 14); "You spend half of your time trying to figure out how it works electronically. You get to keep relearning new things."(no 3). Et aussi, "jouer avec l'ordinateur est un hobby. J'investis du temps personnel pour apprendre" (no 17). Enfin, "je mets beaucoup de temps à aider les collègues à trouver des affaires. On apprend les uns des autres" (no 25).

Enfin, la troisième remarque se situe comme le pendant à la remarque précédente. S'il est vrai qu'une période d'ajustement est vécue et peut être nécessaire, des solutions idoines sont mises sur pied après coup à défaut d'avoir fait partie d'une planification stratégique, pour régler en partie le problème vu comme très ennuyant par les policiers. Ainsi, "de plus en plus des unités spécialisées sont mises sur pied non seulement pour donner un coup de main dans la compréhension des outils mais aussi dans les utilisations efficientes" (no 8). Comme on nous l'a souligné, et il est bon de le noter ici, "on a une section qui nous assiste lors des perquisitions pour récupérer les données" (no 12).

2.1- Les pratiques d'enquêtes de la criminalité

Au niveau des policiers de première ligne, l'arrivée et l'utilisation des banques de données comme le Centre d'information de la police canadienne a permis une amélioration de la mise en application des lois sur les véhicules automobiles. La performance des policiers s'en est trouvée améliorée. Par contre, l'introduction d'outils technologiques plus performants au niveau des enquêteurs ou des gestionnaires reste nettement plus remise en question. Benson (1993) nous rappelle, par exemple, que la plupart des crimes en Grande-Bretagne n'ont pas été résolus par l'introduction du système HOLMES (Home Office Large Major Enquiry System) qui voulait établir des standards dans les renseignements à recueillir et à colliger.

Par rapport aux pratiques d'enquêtes et d'analyses, les technologies de l'information restent encore à ce moment-ci des outils de travail vus comme relativement nouveaux et menaçants. En effet, décrits il y a quelques années comme "des bébelles" par un gestionnaire d'une unité d'enquête, il reste que certains se

demandent encore qui devrait utiliser les technologies et quels enquêteurs devraient y avoir accès, surtout dans le domaine de la cyber-criminalité. Comme nous l'avions constaté précédemment, les technologies de l'information ont commencé à s'infiltrer dans la police d'une façon hiératique et rarement planifiée. Les policiers sont confrontés à des criminels qui sont plus habiles et comprennent mieux le langage des ordinateurs et des technologies. Ils souffrent aussi d'une absence de formation adéquate et au bon moment. De plus, à cause du manque d'expertise ou du manque de formation, ils sont appelés à demander de l'assistance extérieure à des compagnies spécialisées ou à un des experts travaillant pour le service. De plus, le domaine des technologies change tellement rapidement qu'il est difficile pour les policiers et pour les organisations de se tenir à jour. On nous a aussi mentionné le manque d'équipements ou d'équipements adéquats ainsi que la somme de temps à consacrer pour mener des enquêtes rigoureuses (LeBeuf, 2000a, 2000b).

Il en découle toutes sortes de conséquences à divers niveaux. Une première importante et déterminante est qu'avant de se demander comment les policiers, les enquêteurs et les analystes utilisent les technologies mises à leur disposition, il aurait fallu préparer l'environnement policier aux grands bouleversements provoqués par les technologies. Or, cette période mitoyenne d'acclimatation nécessaire est soit complètement niée par des commentaires comme: "tu t'amuses avec ça (ordinateur)" (no 13), ou peu comprise. Dans ce cas, la technologie apparaît comme une menace qui serait vaincue seulement par les initiés: "la peur de la technologie rend les enquêteurs aveugles..."(no 19).

Une seconde conséquence est directement liée à l'usage ou à l'utilisation réelle ou souhaitable qui en est faite. Encore ici, les changements profonds et inévitables provoqués dans les pratiques des policiers sont trop souvent évacués par manque de préparation. Une remarque intéressante à cet effet: un gestionnaire constatait que plusieurs enquêteurs n'utilisaient pas ou peu les ordinateurs mis à leur disposition soit pour rédiger leurs rapports soit pour rédiger les mandats de perquisition: "Les gars rédigent des affidavits et vont le faire à la main parce qu'ils n'ont pas le doigté. Le copier/coller n'est pas maîtrisé par tout le monde. Il fait réellement le copier-coller physiquement et le donne à une secrétaire" (no 13). Et un autre gestionnaire ajoutait sur le même thème : "je veux qu'ils apprennent à travailler avec les ordinateurs. Je ne veux pas que ça soit leur femme qui remplissent les rapports à la maison. Ca va changer parce que les gars vont devoir s'asseoir et rentrer leur information...."(no 4).

Les conceptions de l'usage réel des technologies est qu'il y a définitivement un besoin pour ces outils.

Comme il a été correctement souligné: "les Hell's ont des courriers électroniques, des sites web. On en a besoin nous aussi" (no 10). Ce besoin demeure tributaire en partie de l'accès aux outils, d'un accès facile, d'aucuns diront "*user friendly*" (no 26), et immédiat selon les besoins. Nombreux ont été les enquêteurs à déclarer qu'ils n'avaient pas leur propre poste de travail. Selon l'unité, le ratio est dit-on, un ordinateur pour six personnes, ou pour quatre. "Ici on manque d'ordinateurs. Il faut passer à notre tour ou attendre une ou deux heures" (no 22). Un service de police comme la GRC par contre fournit le matériel nécessaire à l'ensemble de son personnel d'enquête et d'analyse.

Il découle de ces constats que les pratiques d'enquête et d'analyse sont directement influencées. En effet, l'accès direct engendre des pratiques d'usage où le recours à l'ordinateur, et par là aux banques de données informatisées, devient systématique selon la section à laquelle on appartient. Le contraire est aussi vrai. "Les technologies ici ça se développe lentement...Là où j'étais avant c'était un automatisme d'aller voir les banques de données. Alors qu'ici non" (no 9).

Par ailleurs, un gestionnaire d'unité mixte discutant des outils technologiques fournis à son personnel remarquait qu'aucun de ses membres n'avait son ordinateur personnel. Pour lui: "ma job est de prouver qu'ils (membres du crime organisé) font du trafic de drogue pas de jouer avec l'ordinateur...si tu as besoin de support pour aller chercher ta preuve, prends les démarches pour l'obtenir" (no 7). Ce rapport aux technologies illustre en partie les difficultés que les enquêteurs rencontrent au quotidien avce l'usage des technologies. Par exemple, un policier d'une unité du crime économique confiait qu'il était le seul à avoir développé une expertise dans la connaissance et l'usage des technologies de l'information: "je suis le seul à avoir produit ma preuve sur CD-ROM, 80 000 pages de documents et annexes sur deux CD-ROM. C'est une première au crime économique. On a scanné le papier et des liens hyper textes sont possibles. Mon cahier d'enquête est informatisé. Avant tout était à la main. Depuis trois ans le mien est informatisé" (no 5).

Le développement du personnel et d'une expertise appropriée pour certains, incluant les enquêteurs, font désormais partie de l'évolution de la police. L'expertise est d'autant plus nécessaire comme dans les domaines reliés aux technologies où les policiers avouent d'emblée ne pas être prêts à enquêter, soit qu'ils ignorent l'usage des technologies comme l'accès à Internet par exemple, ou encore qu'ils ne sont pas en mesure d'en évaluer la portée. Les arguments s'énoncent ainsi: Pour "les crimes en émergence on est pas équipés, pas formés et on n'a pas d'outils. Il y a un gros manque on le critique" (no 21). Et, "on

n'est pas prêt à les travailler, on n'a pas les compétences pour être efficaces dans ce type d'enquête" (no 22). Ou encore, "les cyber-crimes et e-commerce si on reste dans nos juridictions on y arrivera jamais. C'est l'enfer. On doit travailler d'une façon plus globale" (no 5). On le voit, l'expertise est nécessaire. Or, le développement de l'expertise de pointe entraîne à son tour des difficultés majeures pour la police, difficultés dues à la mobilité du personnel. Les processus de promotion fonctionnent de telle sorte qu'un individu même hautement formé doit quitter la plupart du temps, (il y a quelques exceptions), son champ de compétence pour accéder à une promotion. Lorsque l'individu quitte sa fonction, il en découle une perte d'expertise, sans mentionner les individus qui quittent pour l'entreprise privée pour une période de temps souvent longue, au cours de laquelle il faudra combler le poste. Pour un gestionnaire "la mobilité du personnel est la plus grande difficulté. Il y a perte d'expertise et le temps pour combler des postes est long....je ne les aurai pas avant cinq mois..."(no 4). Pour un gestionnaire d'unité mixte, "avec les promotions on les perd. On n'est pas capable de garder notre expertise" (no 7). Et aussi, "il y a un roulement chez les policiers. Ça prend une stabilité dans le domaine" (no 17). Le développement d'experts de pointe entraîne aussi comme effet que lorsque l'individu quitte c'est toutes les fonctions spécialisées qui s'en vont. Un expert parlant de ses fonctions constatait ceci: "Il n'y a que moi qui ai des contacts. Le jour où je ne suis plus là, il n'y a plus de contacts. Le point de chute est un gros problème" (no 19).

Une des conséquences inattendues de l'arrivée et de l'usage des technologies se reflète dans une nouvelle distribution du travail. Ainsi, ce n'est pas tant le genre de travail qui est modifié que la somme de travail demandée et les étapes subséquentes. Ce sont aussi les étapes relatives à la collecte des informations et à leur mise en banque qui apparaissent comme un supplément dans la tâche. A cet effet, on a dit "avec la technologie on n'est pas efficace. Le travail devrait être plus efficace mais la tâche est augmentée" (no 15). Et, "on est de moins en moins à faire de plus en plus de travail" (no 19). Et aussi, "police officer are put to computer processing date in day out. It is a total waste. We need civilian doing those jobs"(nos 14, 30).

Que sera l'avenir dans le domaine? Certains parlent de patrouille virtuelle du *net* comme elle se pratique entre autres mais pas exclusivement par le *FBI, le U.S. Secret Service, le Customs Service*, comparant la patrouille traditionnelle de rue avec les crimes potentiels commis par le biais de l'ordinateur (Sullivan, 1999). Pour certains services de police au pays, "la vigie sur le net est dans nos plans" (no 8). Certains autres avouent qu'ils utilisent les logiciels, et donc les outils qu'ils connaissent, et ont peu de curiosité pour

se familiariser avec d'autres outils. Pourtant le développement dans ce domaine se fait à un rythme très rapide. "Nous on travaille avec les logiciels que l'on connaît...certains sont devenus des outils pour gérer mieux et plus rapide...mais les enquêteurs ont mal réagi (no 5).

En bref, il est faux de prétendre que les technologies seraient reliées à une question d'âge chronologique ou d'années de services. C'est surtout une question d'attitudes à développer. Par ailleurs, il est normal qu'il existe une période de flottement dans l'apprentissage individuelle ou par programme de formation et dans l'aide à donner aux collègues. Cette période est vue comme une perte de temps, comme un manque d'efficacité dans la tâche. Enfin, des services spécialisés sont de plus en plus développés pour aider les policiers dans les fonctions reliées à la saisie de disques durs d'ordinateurs par exemple.

Le manque de préparation de l'environnement policier à l'arrivée et à l'implantation partielle des technologies a entraîné certaines conséquences comme nier la période de flottement nécessaire suivant l'arrivée d'outils complètement novateurs pour la police. Une autre conséquence est de vouloir forcer les individus à adopter de nouvelles pratiques avant d'avoir été entraînés à le faire.

Les pratiques d'enquêtes sont influencées par l'accès direct aux outils technologiques comme l'ordinateur, par les possibilités encore peu utilisées de se servir du potentiel des outils comme le *CD-ROM.* Il faut non seulement continuer d'éveiller la curiosité des individus mais il faut aussi favoriser leur épanouissement.

Enfin, la police est constamment confrontée à mobiliser son personnel pour de nouvelles formations due au fait que le système de promotion amène les individus à quitter leur champ d'expertise.

2.2- Les méthodes d'enquête

Si, comme nous le prétendons, les enquêteurs ont en général une vision trop limitée dans le cours d'une enquête, il apparaît qu'il faut se pencher directement sur les représentations qu'ils ont de leur métier. Nous nous sommes particulièrement intéressé à la segmentation traditionnelle qui existe dans le monde des enquêtes par la création des différentes unités afin de mener plus efficacement une enquête. Ces unités, illustrées par exemple par les unités de crime économique, de crime contre la personne, des stupéfiants etc, ne favorisent par les contacts entre les policiers soit par tradition ou par apprentissage à la

culture professionnelle. Un patron d'enquêtes a résumé une certaine façon de comprendre l'approche la plus traditionnelle dans les enquêtes en soulignant ceci : "...la nature du crime est simple à comprendre, la prouver est autre chose. Que l'on mette à sa disposition les outils dont il a besoin. On va obtenir les résultats voulus" (29).

Trois constats s'imposent à ce moment-ci. Le domaine des enquêtes semble souffrir du syndrome de l'action immédiate. Les méthodes de recherche informatisées ayant recours à divers logiciels sont encore peu valorisées. Comme le soulignait un patron d'une unité d'enquête importante, "les enquêteurs ne voient pas l'importance d'aller fouiller dans les banques de données. ....tu ne trouveras jamais de bandits là-dedans" (no 13).

Le domaine des enquêtes ne suit donc pas la progression de la criminalité. S'il en était ainsi, "on changerait au fur et à mesure des années comme le crime organisé" (no 22), ce qui ne se fait pas. Une proposition pour remédier à cette situation serait de débuter une enquête à partir de l'analyse de renseignements afin de structurer la stratégie à adopter. Trop souvent, dit-on, "on commence par le bas, par des enquêteurs qui ont une source et qui pensent qu'on va aller attaquer le king pin de....on dépense beaucoup d'argent là-dessus pour rien" (no 15).

Enfin, le recours aux technologies de l'information pour diriger une enquête et pour la collecte et la gestion des informations fait désormais partie des outils disponibles pour les policiers. Des enquêteurs ont soumis les éléments de preuve sur un *DVD*. Le juge, les procureurs de la couronne, les avocats de la défense ont bien réagi. Depuis, dit-on, "on a plus de demandes pour présenter la preuve de cette façon-là surtout dans des dossiers d'envergure" (no 8). Paradoxalement, des enquêteurs et des analystes reconnaissent que les "enquêteurs en général sont peu habiles et pas intéressés à structurer les infos avec ces outils là...mais ça s'apprend" (No 24). Ils seront de plus en plus nombreux toutefois à être confrontés dans un avenir prochain au temps réel du fonctionnement des technologies. Ils réaliseront également l'ampleur du problème causé par l'abolition des frontières, mais non pas des lois à l'intérieur de celles-ci . Enfin, viendra le jour où dans le cadre de la structuration d'une enquête régulière il faudra se demander quelle est la portion d'enquête traditionnelle et la portion d'enquête technologique : "il faut être capable d'enquêter, capable d'aller chercher les éléments majeurs sans faire du technique" (no 19). Ceci représente un des grands défis de la police.

Les unités d'enquêtes, telles que constituées présentements créent un cloisonnement entre les membres. Plusieurs ont reconnu que le cloisonnement réel est nécessaire. De plus, il faut qu'il soit maintenu ainsi. L'argument est que les ressources nécessaires, les habiletés d'enquête et les façons de faire avec les procureurs sont spécifiques à un type d'enquête. "Les ressources ne sont pas les mêmes pour les homicides que pour les stupéfiants. Chaque champ d'activités a ses spécialités, les procureurs de la couronne, la jurisprudence" (no 4). Ou encore, "il y a des choses très spécifiques à une enquête qu'il faut savoir" (no 20). Plus globalement, on s'entendrait pour dire "on a toujours besoin de bâtir des compétences dédiées aux stupéfiants ou ailleurs et de donner des services dans chacun des secteurs spécifiques (no 11).

La recherche et le maintien de l'expertise dans les enquêtes sont importants et pour plusieurs primordiaux. En effet, l'expertise égale compétence dans la façon de mener une enquête. Comme on le faisait remarquer, " we live in a world of specialty...the courts have been making such voluminous decisions. There are so much case law and so much new development and interpretation in the last 15 years it has forced police forces to have specialists. So they say you focus on homicide that is because it is your speciality and you are really good at doing homicide .....if you can't carry your specialty your team will fail"(no 27).

À l'opposé, il y a l'absence d'expertise où "être généraliste" équivaudrait à l'absence de compétence. Comme le disait un enquêteur: "plus tu es généraliste moins tu es bon. Tu es bon pour tout faire mais rien en profondeur.....Il est important d'avoir des spécialistes" (no 17). D'ailleurs, cette opinion est partagée par plusieurs des personnes rencontrées pour qui le domaine des enquêtes demande présentement"de développer des habiletés particulières et très spécialisées. Ce n'est pas vrai qu'un enquêteur est bon en tout" (no 13). De plus, ces habiletés sont nécessaires dans le cadre du développement des lois, comme la Charte canadienne des droits et libertés, de la jurisprudence qui rendent les enquêtes plus complexes et plus exigeantes. Il est primordial alors que "les gens développent une expertise, en même temps qu'il puissent élargir leur horizon" (nos 1, 3). Il y a également les enquêtes à volet international qui exigent une expertise de pointe et des compétences spécifiques. La criminalité transnationale exige de nouvelles compétences. "Today it is transnational. So in order for an investigator to be effective he does not need to learn only about the laws in Canada. He needs to know those of China, etc" (no 3).

Les analystes de la criminalité représentent une catégorie spéciale d'experts dans le domaine des

enquêtes. On retrouve deux types d'analystes, des civils ou fonctionnaires et des policiers analystes. L'avantage du deuxième type est, dit-on, "qu'il est plus facile pour un policier de comprendre les commandes à travers le langage utilisé" (no 6). L'inconvénient de ce type, par contre, est qu'il y a un haut taux de rotation parmi ces derniers, le travail d'analyste étant "un tremplin pour autre chose dans le service" (no 24). Globalement, on peut dire que les opinions à l'égard des analystes est qu'ils font partie de la dynamique des enquêtes. Dû au fait que plusieurs des analystes sont du personnel civil, on considère "qu'ils créent une dynamique qui fait avancer les enquêteurs, entre autres parce qu'ils ont une façon de penser différente des policiers" (no 1). On dit aussi qu'ils apportent une contribution particulière. La contribution s'illustre de différentes façons quel que soit le domaine d'enquête dans lequel ils travaillent. D'abord on dit qu'ils structurent "le matériel d'un dossier pour pouvoir se rendre à la cour" (no 8). Ils créent avec des logiciels des *hyper-liens* entre les informations liens qui ne pourraient être faits par les enquêteurs qui "ne connaissent rien aux technologies"(no 23). Aussi "ils ne savent pas le faire. Ils vont cueillir de l'info et me la donne et me disent, fais-le" (no 6). Ils jettent aussi un nouvel éclairage sur l'enquête qui peut permettre quelquefois de réorienter sur des éléments non retenus (no 25). La contribution peut être aussi dans la direction que peut prendre une enquête. Un analyste prétendait ceci: "la tendance veut que l'analyste dirige plus l'enquête. Tu vas dire à ton enquêteur que c'est comme ca, toujours en pensant à l'information que nous avons"
(no 6). Une dernière note: il apparaît que les analystes n'ont pas la préoccupation d'échanger des informations. Ils confient qu'ils ont des champs de compétence particuliers qui ne favorisent pas les contacts et les échanges (no 23, 14).

Toutefois, la nécessité de travailler en cloisonnement et avec des experts engendre un certain nombre de problèmes. Par exemple, il est reconnu qu'une telle façon de fonctionner engendre la compétition entre les unités d'un même service de police (no 16). Certaines unités semblent avoir une situation plus enviable, du moins plus visible de l'extérieur. Ceci crée un véritable problème au niveau de l'expertise développée dans les unités, expertise qui peut se perdre quand les individus sont attirés par des unités plus "glorieuses". De plus, la compétition s'illustre dans la gestion des enquêtes au quotidien. Si, lors d'une enquête, des éléments sont reliés disons au crime organisé, des enquêteurs disent alors "qu'ils feront les liens nécessaires" et se mettront en contact avec les collègues. "On leur donnera des hints" (no 12). Mais il apparaît que ces contacts ne seront pas faits systématiquement. Il semble que la vraie question non débattue est de savoir finalement "qui va prendre le dossier si ce n'est plus la personne" (unité des crimes contre la personne) (no 6), ou autrement dit, quelle sera l'unité qui va s'occuper

officiellement de la gestion de l'enquête et de ses résultats?

Existe-t-il une hiérarchie informelle entre les unités dans la police? A cette question, la réponse est définitivement oui. Les motifs de cette perception deviennent extrêmement intéressants à décliner. Il y a, dit-on, des crimes qui peuvent être utilisés au maximum. "Certains types de criminalité s'y prêtent plus, il y a du sang, beaucoup de publicité.....tu ne vois pas la même chose selon où tu es assigné dans la police" (no 9). De plus, comme l'avait noté un enquêteur dans le domaine des opérations "tes qualités se mesurent aux résultats obtenus". Cette attitude, discutable en soi, crée un sentiment d'urgence mais aussi suscite nécessairement de s'engager dans des actions ponctuelles. Et, de fait, certaines unités de par leurs activités très médiatisées, créent des envieux : "Les gestionnaires ont accepté que les enquêteurs dans le crime organisé vont plus vite et demandent plus de temps supplémentaire. Ils ont des budgets parce que les prises sont très grosses" (no 16). Il arrive que des membres d'unités conjointes soient vus comme cherchant à tout prix à rendre leurs actions publiques, une publicité qui amènerait par la suite des bénéfices secondaires comme des budgets plus importants, des téléphones cellulaires et des ordinateurs pour tout le personnel. On a dit :"they have more money, there is a lot of rivalry" (no 14). Et aussi, "quand des gens viennent de ces unités ils ont tendance à court-circuiter les autres parce qu'ils veulent être sur la sellette" (no 22). A l'inverse, les membres d'unités qui ne sont pas dans l'action sont perçus comme moins importants et n'attireraient pas autant de nouveaux équipiers. De là, cette remarque, "au crime économique on prend qui veut venir et au crime contre la personne on prend qui on veut" (no 17). Le commentaire d'un enquêteur d'une unité du crime économique illustre bien la situation : "à l'interne on est des brasseux de papier on n'est pas dans l'action. À l'externe, ils nous voient comme des professionnels" (no 4).

En bref, il existe un cloisonnement réel et nécessaire entre les unités d'enquête. Ce cloisonnement est le résultat d'une expertise de pointe développée pour rencontrer les difficultés particulières des enquêtes.

Le cloisonnement engendre une compétition remarquée entre les unités, certaines ayant un impact public très grand. Le cloisonnement favorise aussi une expertise de pointe dans un secteur donné.

Une catégorie d'experts dans le domaine des enquêtes est celle des analystes. Les enquêteurs en ont besoin. Ils contribuent tout particulièrement au plan de la gestion des informations complexes, au plan de l'orientation d'une enquête et aussi au plan de la compréhension des divers éléments reliés à l'enquête.

Il existe une hiérarchie formelle entre les unités d'enquête. Cela entraîne des conséquences au plan de la publicité accordée, des budgets importants obtenus, des outils comme les téléphones cellulaires, ordinateurs, *pagettes,* etc. accordés à tous les membres de ces unités.

Le domaine des enquêtes, domaine pivot s'il en est un dans la police, accepte le changement nécessaire à pas de tortue. Les méthodes d'enquête gagneraient à être approchées de manière plus dynamique ou divers éléments jouent à la fois dans la stabilité des manières habituelles de travailler et dans d'autres plus novatrices. Cette dynamique implique justement qu'il y a des façons de faire dans les enquêtes qui seraient plus pertinentes ou plus adaptées à la réalité de la criminalité des années 2000.

2.2.1- Les unités mixtes d'intervention contre les crimes

Une unité d'enquête particulière concerne les unités mixtes d'intervention contre les crimes. Les unités mixtes rassemblent des policiers de divers services de police et aussi, selon le cas, des agents d'application de la loi d'organismes comme l'Agence canadienne des douanes et du revenu, etc. L'objectif est de rassembler les forces communes pour combatte le crime organisé, par exemple. Ce type d'initiative est né à partir de trois grands constats reliés, mais pas toujours bien identifiés, à savoir:

- "qu'un seul service de police n'est pas en mesure de combattre le crime seul" (no 11),
- "trop souvent certaines unités de service de police travaillaient en vase clos sans utiliser les ressources et les informations des collègues" (no 7)
- les ressources financières nécessaires sont importantes. Or, peu de gouvernements ont habituellement de nouvelles sommes à investir (no 7)

Les unités mixtes ne sont pas nouvelles. Par exemple, depuis au moins 15 ans, la GRC a mis sur pied de telles unités pour combattre les drogues dans le port de Vancouver. Présentement, toutefois, elles sont davantage en expansion. Certaines sont formées sur une base permanente, d'autres sur une base plus ponctuelle. On retrouve des équipes mixtes pour combattre le crime organisé dans la grande région de Toronto, le Groupe spécial interpolice mieux connu sous son acronyme anglais CFSEU (Hamilton, 2000), ou dans le domaine du renseignement par l'intégration d'unités de renseignements de services de police indépendants qui regroupent des enquêteurs et des analystes. On peut aussi concevoir la mise en place de partenariats avec de grandes corporations comme les sections d'enquêtes du Canadien National, par exemple, ou encore de l'industrie des banques.

Au moins trois facteurs contributifs ont été identifiés. D'abord, les unités mixtes sont décrites comme de nouvelles approches du travail de la police dans le sens suivant. Comme les services se retrouvent "tous à la même table", les efforts de la police sont unifiés (nos 20, 10, 30): "I always found that JFO are the best way to go " (no 28). Ajoutons ici que l'unification des efforts cause un certain nombre de problèmes reliés à la philosophie de travail, à la formation de base et au programme de formation continue, aux conditions et horaires de travail, aux politiques d'encadrement, aux budgets disponibles. Par ailleurs, l'unification des efforts facilite une meilleure coordination des moyens d'action disponibles, des moyens d'enquête et des budgets par rapport à une cible précise. Ainsi, c'est moins l'individu que l'organisation qui devient l'enjeu réel de la mise en application de la loi. Il est dit aussi qu'un travail en collaboration favorise pour plusieurs policiers et policières, une ouverture de leurs horizons et de leurs préoccupations (no 1). À ce moment-ci, ce sont davantage les valeurs culturelles propres à chaque service de police qui sont mises au défi.

Quant au second facteur contributif, il est considéré que les unités mixtes ou en tout cas le travail en groupe conjoint est dorénavant la façon de faire de la police du XXI ième siècle. Ainsi "les équipes multi-disciplinaires composées de spécialistes de différents secteurs d'enquête sont la meilleure adaptation que l'on a pu penser pour l'instant. Ça permet de joindre des gens qui ont des connaissances différentes, précises et spécialisées dans divers domaines...Les équipes sont une modification des anciennes façons de faire. On s'éloigne des mandats précis où on n'attaque plus en fonction d'un mandat mais d'un groupe" (no 29). Le ralliement d'une partie des forces permet donc des alliances ponctuelles et relativement efficaces (no 2). Ce type d'alliances fait en sorte que les individus deviennent moins préoccupés par leur propre sphère d'influence (turf) et centrés davantage sur les cibles à combattre. De même, l'union d'une partie des forces fait en sorte que l'aide ponctuelle pour des opérations précises est facile et rapide à obtenir étant donné les contacts formels déjà établis (no 14). En fin de compte, la police devient théoriquement plus efficace parce qu'il n'y a pas duplication des forces et des énergies sur les cibles.

Un troisième facteur, déjà mentionné, est à l'effet que les unités mixtes ont comme résultat de proposer des moyens d'intervention qui, rassemblés sous une même bannière, permettent de donner un coup de main à des unités ou à des services qui n'ont pas le temps ou qui ne sont pas équipés pour le faire (no 6, 11). Il en découle également que les policiers des services de moyenne et de petite taille bénéficient

beaucoup de ce type d'échange par leur apprentissage des moyens, des techniques de travail, des approches en résolution de problèmes et par le choc des valeurs culturelles des services en présence. Il s'installe également une complicité entre les individus quelle que soit leur appartenance initiale, complicité qui devient une valeur ajoutée pour la police (no 23).

Par ailleurs, il faut mentionner un certain nombre d'inconvénients qui apparaissent aux yeux de plusieurs plusieurs comme des problèmes à résoudre dans la marche vers le succès des unités mixtes. Au moins deux ont été identifiés. Le premier porte sur les habiletés et compétences des individus en présence. Dans un contexte où les législations et les procédures sont complexes, il apparaît directement que les compétences des individus ne sont pas toutes au même niveau. Non seulement le type de formation n'est pas identique mais les habiletés développées ne sont pas toujours comparables : "the partners are excellent but their training is very different than peace officers" (no 14). De plus, dans un contexte où existe cette peur que "les gros (services) prennent toute la place" (no 2), les expériences passées et les connaissances développées jouent à plusieurs niveaux, entre autres contre les services de petite taille. Les procédures complexes, la philosophie d'enquête, la ligne hiérarchique (reporting structure) peuvent faire en sorte qu'une unité soit moins efficace qu'elle ne pourrait l'être autrement (no 14). Enfin, il existe toujours la possibilité qu'une rivalité s'installe entre les membres des équipes. Dans ce cas, le projet peut potentiellement être menacé, d'où cette remarque : "you can lead a horse to water you can't make it drink. You have to convince people that is the right thing to do" (no 27).

Le second problème concerne la gestion des unités. Vue comme un problème structurel, la question soulevée se présente ainsi pour un gestionnaire : comment arriver à bâtir une vraie équipe centrée sur le même but (agenda). "It goes to the personalities of the team leaders....if he can it will work relatively well. If he can't then that is where problems start to..."(no3). Cette question se pose en plus dans un contexte où les individus des organismes prêtés ne se rapportent pas au chef d'équipe pour leur évaluation annuelle, leurs congés, etc: "None of them is answering to you for performance review, assessment or anything. You may have a say if the supervisor asks. The team leader has responsibility for the day to day. " (no 14).

En bref, les unités mixtes apparaissent comme des moyens efficaces et relativement nouveaux de combattre le crime. Elles permettent d'unir des moyens d'enquête, des budgets, des outils d'application de la loi et des individus dans un but commun. Ainsi elles contreviennent aux menaces de duplication des

forces dans un univers en mutation constante.

Par leur existence, les unités favorisent également des alliances ponctuelles et des contacts privilégiés entre individus et entre les organisations. Il en découle que les demandes d'aide sont grandement facilitées.

Les freins à l'efficacité attendue des unités est la disparité des valeurs culturelles entre les organisations, mais également les questions des bénéfices marginaux, les procédures complexes, la philosophie d'enquête, la ligne hiérarchique, la philosophie de travail, la formation de base et les programmes de formation continue, les conditions et horaires de travail, les politiques d'encadrement et les budgets disponibles. Par contre, un élément majeur concerne le partage des informations.

3- Le renseignement et ses usages

Les informations contenues dans les banques de données informatisées et les dossiers constituent des outils de travail, pour les enquêtes en particulier. Un renseignement d'appoint orientera les cibles les plus favorables pour des opérations policières efficaces. Il devient important alors de savoir dans quels buts les informations sont colligées, surtout dans le combat contre le crime organisé. Poser la question montre qu'il n'y a pas de position uniforme quant aux buts poursuivis. On peut penser que des programmes de formation déficients, ou l'absence de formation adéquate ou de formation tout court, explique la disparité des buts mentionnés plus bas.

Etant donné qu'un des éléments moteurs de cette recherche est le crime organisé, nous pensons qu'il est intéressant de faire ressortir quelques-unes des perceptions des interviewés. A cet égard, une des personnes rencontrées avait très bien résumé l'état de la question : "... when you use the word organized crime the definition itself means different things to different people depending who you are talking to: the business community, the general community, small police departments, large police departments, the banking community. It has a different face for everyone" (no 2). Cette difficulté de s'entendre sur une définition simple et identique pour l'ensemble de la société sur ce que représente le problème (no 2) a comme effet que la planification de la lutte au crime organisé et l'actualisation engendrent à leur tour des commentaires complexes. Par exemple : "quand tu attaques quelque chose en regardant le renseignement criminel forcément tu ignores autre chose. On attaque un groupe comme les motards. Ça

veut dire que les autochtones, les Italiens, Eastern European, les Jamaicans débarquent. Si on maintient le cap dans une direction ça va créer d'autres problèmes et indirectement forcer la main aux élus et montrer aux élus que l'on n'a pas forcément tous les outils nécessaires pour attaquer le crime organisé" (no 1).

Ou ceci : "Le crime organisé est un beau chapeau. C'est vendeur" (no 4). Ou encore: "la menta!ité du crime organisé est un informateur, une bonne information, je sors le mandat de perquisition je défonce la porte et j'accuse. Eux le papier ça ne les intéresse pas" (no 5).

Il y a aussi une impression de peur et de menace non contrôlées de la part de la police. Cette peur semble alimentée moins par des informations solides que par des perceptions du sens commun. Ainsi ils ont dit : "ils sont bien organisés. Ils ont des ramifications partout. Plus ça va plus c'est organisé" (no 10). Ou encore, "on se sent dépassés, préoccupés. Ça coûte très cher de faire la police. ...on ne travaille pas à arme égale...on n'a pas les mêmes budgets ni les mêmes règles"(no 9). Ou "les techniques d'enquêtes pour la divulgation de la preuve ont pris de l'ampleur et les bandits les connaissent" (no 12).

3.1- Les buts de la collecte des informations policières

Il y a autant de buts que de priorités selon les enquêteurs rencontrés. Nous les avons rassemblés en trois catégories mutuellement inclusives. Avant de les mentionner, arrêtons-nous au constat suivant à l'effet que la majorité des personnes rencontrées s'entendraient pour dire que les informations sont décrites comme des outils à l'enquête : "Info is a tool to get business done" (no 3). Elles ne constituent pas des renseignements précis mais elles devraient orienter les démarches des enquêteurs. Par exemple, un enquêteur constatait : "l'info est dry-ça sert pour des enquêtes. Ça donne un bon in sur une personne. Quand tu arrives dans un détachement ça te prend un ou deux ans à connaître ton monde. Si on avait eu une banque de données tu pitonnes et tu as le background de tous les gars qui ont travaillé avant toi" (no 18).

Une fois ce premier constat fait, arrêtons-nous au trois catégories de buts et de priorités.

Dans la première catégorie, les informations servent de guide soit pour orienter une enquête, ou soit pour orienter les policiers. En ce sens, elles indiquent par exemple l'usage de véhicules, identifient des

personnes, ou les délits antérieurs, les enquêtes. Si l'information est contemporaine, elle devient pertinente pour alimenter un dossier. De même, constatant que "ce n'est pas vrai que l'info bénéficie à tout le monde" (no 16). Une personne ajoutait: "quand tu débutes une enquête sur un individu pour essayer de voir ce qui a été fait. Ça te permet d'entrer en communication avec les enquêteurs qui ont déjà travaillé. Plus les services sont gros plus ils bénéficient du renseignement"(no 16). En ce sens, les informations ne servent pas à "faire des mandats mais à voir si tu es sur la bonne piste" (no 13).

Pour d'autres, "quand les policiers auraient les infos en main, elles leurs permettraient de prendre des décisions éclairées et solides"(no 1). Mais, ajoutait-il, "ils ne les ont pas en mains présentement les informations". L'impact de telles décisions serait pour les policiers d'apprendre à moins focaliser sur des individus que sur les groupes ou sur les organisations auxquelles ils appartiennent, surtout les membres du crime organisé (no 3). En fait, ici c'est la culture des enquêtes qui est à repenser. Nous y reviendrons.

Dans la seconde catégorie, les informations servent à améliorer la qualité des opérations, à établir une stratégie et à permettre des analyses poussées. En soulignant que le renseignement est "le nerf de la guerre" un enquêteur faisait ressortir que le renseignement aide à "réduire l'entonnoir pour pointer là où est le crime, l'endroit, le moment, etc. Il permet en fait d'être en avant des criminels"(no. 7). En fait si les renseignements étaient utilisés selon une stratégie planifiée, des commentaires comme le suivant n'auraient pas lieu d'être formulés de la même façon: "the Hell's Angels , why is it that they continue to function? The answer is when you look at the way we are establishing our priority are been driven by the informant on the street" (no 30).

Dans la troisième catégorie, les informations servent spécifiquement à préparer des affidavits. Comme il était mentionné "tu sais ce que ça prend en enquête pour aller à la cour" (no 6). Ainsi, les renseignements comblent les besoins des enquêteurs et des analystes pour monter des dossiers acceptables et ce dans le respect des législations actuelles.

En bref, on voit que les informations aident l'enquête en général en permettant de se documenter sur l'histoire antérieure des cas, en orientant la poursuite de pistes plus ciblées, et finalement, en facilitant la préparation des documents légaux pour le tribunal. Or, il est sous-entendu que les informations sont non seulement contemporaines mais aussi de qualité.

Toutefois, la qualité et l'usage des informations restent encore à être déterminés. Examinons-les.

3.2- La qualité et l'usage des informations

D'une façon générale, les personnes rencontrées s'entendent pour dire que les informations mises dans les dossiers ou dans des banques de données sont "significatives et veulent dire quelque chose" (no1). Dit autrement, les informations doivent être utilisables, c'est-à-dire fiables, mais surtout contemporaines. L'information devient contemporaine à la lumière des préoccupations d'une enquête. Comme le disait un gestionnaire, "ce n'est pas vrai que les infos bénéficient à tout le monde. Ce qui est vrai aujourd'hui pourrait être faux demain et vice versa. Tout est vrai dans une banque même si c'est inutilisable" (no 16). Toutefois, il est primordial que les enquêteurs aient accès aux informations et aussi qu'ils soient capables de les interpréter, ce qui semble causer de vrais problèmes. En effet, les banques offrent une certaine facilité pour le travail en autant que les individus puissent les manipuler et les interpréter convenablement. Comme le mentionnait à juste titre un gestionnaire d'enquêtes spécialisées, "it is one thing to collect it- what do you do with it, how do you make use of it as a broad picture as guess is the real question" (no 3).

Cette remarque nous renvoie directement à la valeur probante des informations, valeur qui pour plusieurs devrait conduire à des actions ponctuelles telles des arrestations, des condamnations et leur utilisation en preuve.

"Avoir du renseignement c'est bien beau mais quel type de renseignement, des outils utilisables en preuve, qui permettent de procéder à des arrestations et à des condamnations?...la valeur du renseignement est chiffrable en ce sens que renseignement égale résultats. Mais il y a du renseignement qui n'a pas de résultat au bout...alors c'est difficile d'évaluer la valeur de ces infos" (no 7).

De plus, il ressort que même s'il y a beaucoup d'informations disponibles dans les multiples banques de données nationales ou plus locales des services de police, il faut continuer de les alimenter parce que, dit-on, "often critical elements are missing....really key info do not get into the system,.....to filter it out together and to link the events is what is really missing....how do you put it together so it makes senses for your purposes" (no 3). Au moins deux raisons sont avancées pour expliquer cette situation : "we do not have the particular skill sets around and also because our technology has overloaded us with information" (no 3).

Dans le même ordre d'idées, le manque de coordination entre les différents systèmes et incidemment entre les services de police contribuent beaucoup à une qualité déficiente au plan des informations à recueillir (no14). Il peut arriver aussi, à la lumière de l'incertitude quant au fondement des informations : "il y a trop que je ne peux pas divulguer ou qui n'ont pas d'intérêt pour moi alors.... un enquêteur décide de fermer son dossier. Le manque de temps et la charge de travail amène à dire "tu fermes ton dossier, autrement on n'en finirait plus" (no 5).

Enfin, il peut arriver que l'information serve à un usage secondaire comme méthode de relations publiques dans les médias. On dit alors que l'information sert par exemple à "se vanter", à prouver qu'ils sont les meilleurs". Il en découle une "hantise qui dit qu'un tel s'est servi de mon renseignement pour renforcer son ego ou son image " (no 8).

En bref, il émerge une préoccupation quant aux informations : il faut encourager la collecte plus globale des informations. On retient que l'exercice porte moins sur le fait de collecter des informations que sur celui de collecter des informations de qualité. De plus, des informations de qualité conduisent à des actions ponctuelles au plan des arrestations et des condamnations. Dans la mesure du possible, les informations devraient être fiables et contemporaines. Enfin, il apparaît que les informations peuvent être utilisées à des fins secondaires comme de la vantardise de la part de services de police.

3.3- Le partage des informations - mythe ou réalité

Il faut se méfier de ceux qui prétendent que la question de la collecte et du partage des renseignements est la même depuis au moins les années soixante. Ceux-là se méprennent sur les grandes transformations légales (législations et jurisprudence) et culturelles à travers lesquelles les policiers et les organisations ont passé. Il y a également des facteurs reliés au budget et au personnel disponible et mouvant, facteurs que nous ne discuterons pas dans ce rapport.

Le partage des informations est en soi une problématique fondamentale pour la police. Il fait appel aux politiques de coopération entre membres d'un service de police mais également avec les services de police du pays et de l'étranger. A l'heure de la montée fracassante des technologies de l'information qui favorisent les échanges avec l'ensemble de la planète en temps réel, il faut se poser la vraie question relative au partage des informations dans la police.

De quoi parle-t-on? Que partage-t-on? Ce n'est pas toujours bien clair et défini. Ce peuvent être des informations générales, du renseignement analysé en partie, ou encore des rapports de sources ou d'informateurs, etc. Par ailleurs, toutes les enquêtes n'exigent pas le même niveau de partage (no 13) et tout n'est pas utile à partager. Alors, comment parvenir à départager ce qui doit être ou non partagé et comment le favoriser?

A la lumière de nos rencontres et observations, nous dirions qu'il ressort quelques grandes **conventions stéréotypées** non remises en question à l'égard du partage de l'information. Elles circulent dans le domaine des enquêtes et de la police en général. Nous allons les exposer sans les commenter à ce moment-ci. Les conventions stéréotypées sont les suivantes :

1- La sécurité des informations, la confiance entre les individus et les méthodes de travail reposent sur le besoin de savoir comparé au droit de savoir (need to know and right to know).

2- Les policiers gardent leurs informations pour eux. Ils ne mettent qu'une partie des renseignements qu'ils obtiennent dans les dossiers ou les banques de données.

3- Il y a en général une surcharge de travail chez les enquêteurs. Ils manquent de temps pour gérer les sommes phénoménales d'informations étant donné les tâches administratives (préparation des mandats) exigées par les législations et la jurisprudence.

4- Plus les enquêteurs auront de renseignements à leur disposition, meilleurs seront les résultats des enquêtes.

5- Le refus de partager les informations est avant tout un problème qui relève des patrons et des autorités - en d'autres mots, les refus ressembleraient quelquefois à des chicanes politiques.

6- Le refus de partager les informations est la conséquence directe d'un manque de collaboration entres les policiers impliqués. Ils ne mettent pas suffisamment l'épaule à la roue une fois que les ententes formelles sont signées un autre niveau.

7- Le partage des informations relève davantage du volontarisme des individus que de politiques administratives suivies.

Ces conventions stéréotypées possèdent des fondements reliés aux apprentissages et aux pratiques des enquêtes. Elles portent aussi le stigmate de situations passées qui ont laissé des traces difficiles à oublier. Comme le mentionnait un enquêteur, "quand ça arrive une fois ça laisse des traces très longtemps" (no 24). Nous allons à présent exposer les facteurs reliés au non-partage et au partage des informations.

D'emblée, toutes les personnes rencontrées sont tombées d'accord, chacune à leur façon, pour dire que le partage des informations est important en principe. Une fois cela dit, le partage même est soumis à une série de facteurs formels et informels pour protéger les informations, les enquêteurs, les sources ou encore l'enquête comme telle. Selon le contexte et l'enquête, il peut arriver que les renseignements ne soient pas partagés à l'intérieur d'une équipe d'enquête. On peut comprendre alors que les informations ne sont pas rendues disponibles aux membres du service de police, à d'autres services de police au pays et à l'étranger.

En fin de compte, si en principe le partage est souhaitable parce que "transmettre nos infos fait que l'on ne travaille pas sur les mêmes dossiers d'une organisation à l'autre" (no 9), une série de facteurs contribuent au non-partage des informations dans les faits.

3.3.1 Les facteurs de non-partage

Aux moins quatre familles de facteurs ont été identifiées. Nous allons les exposer et les commenter.

La première famille de facteurs est relative à la confiance mutuelle entre les individus et les partenaires. La confiance doit être créée et bâtie entre les individus et entre les organisations. Elle doit aussi être soutenue par tous les niveaux des organisations de sorte que la relation de confiance créée à un niveau ne sera pas annulée par les actions d'individus à un autre niveau. En l'absence de confiance, qui semble au départ la règle générale, les individus sont en général hésitants à donner quoi que ce soit (no 26). La confiance doit être instaurée aussi au niveau des relations que les enquêteurs entretiennent avec les sources, les informateurs. Dans ce cas, le lien créé entre le policier et sa source qui fournit des renseignements repose sur une confiance qui peut être menacée si connue. "Mes contacts, mes

sources, ...il y a un lien de confiance. Si tout était dévoilé ça ne serait plus aussi hermétique. Il faut une discrétion professionnelle, on peut dire je suis prêt à t'aider mais il y a des choses que je veux garder" (no 21).

Ajoutons qu'il n'est pas rare que des enquêteurs obtiennent des informations privilégiées ou encore ont accès à des informations dans des banques de données de services de police avec qui ils travaillent en unités conjointes, parce qu'ils ont créé des contacts et se sont établi une crédibilité qui leur permet de traiter leurs dossiers efficacement. Quand ils quittent leur fonction ou qu'ils laissent l'unité conjointe, les informations cessent de circuler immédiatement.

Une deuxième famille de facteurs repose sur l'aspect légal. Il arrive que des renseignements soient donnés par une tierce partie pour aider le développement d'une enquête. Mais arrive un moment où l'organisation doit retourner à l'agence source pour l'informer qu'elle veut utiliser une partie des informations dans la conduite officielle d'une enquête. Alors, c'est la règle de la tierce partie qui s'impose, ce qui implique que les sources comme les renseignements ne peuvent être dévoilés dans un affidavit si l'agence refuse (no 11, 27). Il y a également les législations sur la vie privée, sur la loi de l'accès à l'information qui limitent ou plutôt circonscrivent les règles du partage et de la protection des renseignements. Enfin, une question émergente et cruciale porte sur le partage des informations avec les agences internationales. Les juridictions ne sont pas identiques comme les pratiques de mise en application de la loi. La vraie question qui demeure sans réponse est la suivante: qui va partager les informations avec les agences internationales (No 11)?

De même, pour certains individus, l'autorité des polices selon la constitution les amène à entrer en contact avec la GRC et à communiquer les informations recueillies. "Si quelqu'un me donne quelque chose qui appartient à la GRC, je me sens l'obligation de la partager avec eux" (no 13).

Une troisième famille relève des méthodes de travail dans le domaine des enquêtes. Cette famille est complexe parce qu'elle fait référence à la fois aux attitudes des individus, aux méthodes apprises par des formations sur le tas avec les collègues et aussi à l'ignorance de la manipulation des systèmes informatisés. Reprenons chacun des éléments.

On constate que des enquêteurs qui n'assument pas leurs responsabilités de partager leurs informations ne savent pas vraiment travailler avec des buts stratégiques (no11) : "We still do not get the intelligence. The drug people not sharing their info with intelligence people, none of them are sharing their intelligence with the intelligence bureau cisc" (no 28). Il se peut qu'ils ne l'aient pas appris ou qu'ils ne voient pas la nécessité de le faire, ce qui est davantage dommageable. Dans ce cas, le rationnel relevant des attitudes et de la culture professionnelle fait dire que "les gens ne se parlent pas - c'est la nature humaine. Le monde est territorial dans leurs affaires professionnelles" (no15). Le partage des informations illustrerait alors la perte de contrôle sur leur travail (leur enquête). D'un autre coté, plus d'un interviewé a mentionné que le renseignement en général représente le pouvoir. Il s'inscrit dès lors comme une "chasse gardée", "des choses dont tu ne veux pas parler" (no 22). Ou bien, "there is a certain percentage of investigators who are very proprietary and protective and selfish with their info. I think it is a minority" (no 27).

À cela il faut ajouter toutefois que les difficultés de partage relèvent pour certains de la confiance préalablement établie avec les sources de renseignements. "Souvent quand on rencontre des sources on bâtit une relation de confiance et ils nous confient des renseignements juste à nous. Ils sous-tendent que je la garde pour moi. Je ne dois pas la partager" (no 13). Dit autrement, les individus donnent leurs informations à des enquêteurs en soumettant que les informations ne circuleront pas. La raison pour obtenir les informations devient l'obstacle pour les partager. La confiance s'instaure et repose en grande partie sur le besoin et le droit de savoir. Pour certains toutefois, "need to know - right to know has been abused for years and years. If we would sit down and analyse in some way the most stuff than could be shared I would like to think that it is only the very small stuff that is so sensitive that may it got to be protected in some way" (no 28). Cette remarque suggère une possibilité de réviser les approches mais surtout les attitudes relatives aux méthodes de travail des enquêteurs.

Enfin, les technologies de l'information sont un dernier élément qui constitue à la fois une source de partage des renseignements et une contrainte au partage. En effet, décrites et mises en place pour favoriser non seulement la collecte mais le partage, les technologies de l'information engendrent des difficultés de manipulation, la non-connaissance des systèmes, l'ignorance des potentiels offerts, la non-compatibilité des systèmes, le non-accès ou l'accès difficile, et deviennent des obstacles majeurs et incontournables : "Les banques de données sont d'accès facile à partir du moment où tu es capable

d'interpréter les banques " (no 17). Les technologies constituent une charnière entre les méthodes de travail comme empêchement et également comme conditions de travail ne permettant toujours d'atteindre les objectifs poursuivis.

Les conditions de travail constituent une quatrième famille. Pour certains ce n'est pas une question de vouloir cacher l'information, c'en est plutôt une relative à des limites physiques pour la consigner. "On a tellement d'informations on en consigne, on en partage, mais il est pas possible de prendre une conversation d'une heure et d'en faire une synthèse...physiquement il y a des limites que tout n'est pas consignable" (no13). De plus, s'ajoute à cette remarque le fait que les tâches des enquêteurs sont lourdes. Ils sont soumis à des échéances telles que les dates à respecter pour les assises au tribunal. Le temps imparti pour aller chercher les informations et les consigner devient un facteur difficile à contrôler. "On est pas vraiment encouragé...à un moment donné on m'a dit écoute on n'a pas le temps de faire les synthèses, on ne les fera pas...à la fin ça n'arrête plus j'ai pas le temps" (no 5, 18).

Aussi, "le gros problème que l'on a est pas la mauvaise volonté des gens c'est le temps nécessaire pour l'alimentation des banques - difficile de convaincre un enquêteur débordé de faire une synthèse de ce qu'il a recueilli et de l'alimenter dans une banque qui va peut être servir demain alors qu'il est déjà en retard sur son rapport pour la cour mercredi. C'est ça la vie" (no 16).

Pour d'autres, "le plus gros problème est la multitude des bases de données : "tout le monde a son petit système" (no 12) et la non-compatibilité de celles-ci. Cela cause des problèmes au plan de l'échange physique du matériel. "Il y a des problèmes au niveau de l'échange parce que les logiciels ne sont pas les mêmes...le transfert de l'information ne se fait pas" (no 23). Il en découle également que "ce ne sont pas les mêmes types de données qui sont colligés; de ce fait ...on ne peut pas s'aider" (no 20).

Ces remarques s'inscrivent toutefois dans un contexte où il est justement souligné par un enquêteur d'un service de police de grande taille que "les informateurs sont informatisés depuis plusieurs années dans mon service; j'ai accès aux sources actives à travers le pays. Ça commence à payer maintenant" (no 20). Un gestionnaire du même service ajoutait plus tard, "si la quantité augmente c'est parce qu'il y a un changement de culture, de compréhension et d'utilisation des infos et des effets. Il faut donner le temps au renseignement de faire son oeuvre. Quand on démontrera aux enquêteurs les résultats que l'on peut

obtenir des informations qu'ils ont contribuées, je pense que ça va venir naturellement" (no 29).

Par ailleurs, il arrive que l'accès à des banques de données pour les membres d'un service soit établi par rapport à divers niveaux de sécurité. L'accès limité relève alors de politiques administratives établies pour assurer la sécurité de la documentation. Ainsi un enquêteur expliquant le contexte d'une unité mixte faisait remarquer que l'accès aux renseignements était limité uniquement aux enquêteurs sur le projet X : "On ne le fait pas par exprès pour faire flancher une enquête. On donne des niveaux de sécurité spécifiques pour des matricules" (no 8).

Enfin, comme déjà mentionné, les systèmes de conservation et les outils technologiques pour le faire ne favorisent pas toujours le partage des informations. D'où ce commentaire important et déterminant pour la qualité des informations mais aussi pour leur gestion ultérieure : "before we can integrate our information, because intelligence is not only info it is a process, before we do that we have to get our own information management together" (no 30). En plus de considérer que "le plus gros problème est la multitude des bases de données car chacun a son petit système" (no15), l'enquêteur "ne prend pas le temps de mettre ses informations dans un système puis dans un autre. Il se dit si je vois que mon info est utile je la mettrai dans la banque" (no 15). Mentionnons également le fait qu'une organisation comme le Service canadien de renseignements criminels (SCRC) reste inconnu pour des policiers.

Une solution proposée par un gestionnaire supérieur consiste à rendre les banques de données disponibles aux personnes concernées. Ainsi, "if NCDB is made available to all, it will take away part of the distrust which is being in policing since I was in policing" (no 28).

En bref, les facteurs qui contribuent à l'absence d'échange et au partage des renseignements sont les suivants :

1- une absence de confiance mutuelle entre les individus et les partenaires;

2- des contraintes liées à des législations et à des ententes ponctuelles entre les parties (MOU);

3- les méthodes de travail dans le domaine des enquêtes qui se réfèrent à la fois aux

attitudes des individus, aux méthodes apprises par des formations sur le tas avec les collègues et aussi à l'ignorance de la manipulation des systèmes informatisés;

4- les conditions de travail relatives à la charge de travail des enquêteurs et au manque de personnel; les politiques administratives relatives aux accès limités (niveau de sécurité) et à la méconnaissance des outils technologiques pour la gestion des quantités d'information phénoménales que doivent gérer les enquêteurs.

3.3.2 Les conditions de partage

D'autres facteurs viennent contrebalancer les difficultés de partage. Il existe différentes conditions de partage. Ces conditions se rapprochent soit d'une philosophie personnelle des individus ou soit d'obligations structurelles. Dans le premier cas, on explique que dans un contexte des unités mixtes des enquêteurs soutiennent qu'il est impensable qu'ils ne dévoilent pas une partie des informations de leur service de police aux collègues des services qui participent à l'unité : "I am not going to hide info from them. I do not keep secret from them. We become ineffective and we loose the trust at the end of the day" (no 14). Or, cette position apparaît davantage comme une philosophie personnelle qu'une politique administrative formelle. De même, au niveau des attitudes personnelles des enquêteurs, on a dit que de participer à des projets conjoints où se retrouvent dans une même équipe des services de police de différentes tailles et avec des bases de données différentes, fait en sorte que l'information circule au besoin. Dans ce cas, l'accès est direct aux banques de données par l'intermédiaire des policiers participants. Si un policier d'un service ne peut avoir accès à la banque de données d'un autre service, le collègue du service en question fournira l'information à la demande. L'alimentation est aussi favorisée. Mais il peut arriver qu'à la dissolution de l'unité des services de police de moindre taille ne puissent avoir accès aux informations qu'ils ont fournies dans le cadre d'une enquête. On comprend alors que l'intérêt de participer à la cueillette et à la conservation des informations puisse causer des difficultés majeures.

De plus, certains enquêteurs expliquent leur position personnelle en soulignant : "je me suis fais des contacts - je les appelle. Mais je ne dis pas mes infos à n'importe qui" (no 20). Cette idée de gérer d'une façon individuelle et personnelle les informations policières semble prégnante à tous les types

d'enquête. Comme on soulignait "le principe de base est de mettre des *infos qui t'appartiennent* dans des banques ....tu décides si tu veux la partager"(no 8) (notre souligné). La possession des informations liée au volontarisme pour les gérer constitue certes des embûches mais elle demeure encore à ce moment-ci partie intégrante de la culture des enquêtes.

Une autre condition relève du moment de la divulgation de la preuve. A ce moment-là, il n'est plus question de cacher les informations qui sont au dossier puisqu'elles seront connues nécessairement des avocats et du tribunal. Alors, comme on le soulignait,"c'est le bon moment de le faire". L'information c'est important de la partager, mais c'est important de le faire au bon moment, lors de la divulgation de la preuve à la défense (no 9). Nous comprenons ici que le partage des informations entre les enquêteurs au moment de l'enquête est relégué au second plan.

Enfin, une dernière condition facilitant le partage est liée, dit-on, au manque de ressources pour mener les enquêtes efficacement. On l'explique ainsi : "tu ne gardes par une info parce que tu sais que tu ne seras pas capable d'en venir à terme pour des raisons budgétaires et de priorités. Finalement, tu la partages. Ce qui était une barrière avant l'est moins maintenant"(no17).

Les conditions ne favorisant pas ou peu le partage des informations constituent les deux facettes du même problème. L'une et l'autre apportent des éléments de compréhension et aussi de solutions. Il faut tout de même convenir que des informations sont échangées si ce n'est que par le biais des grandes banques de données de renseignements comme le Centre d'information de la police canadienne, par exemple. Cela constitue certainement une entreprise importante pour l'application de la loi. Toutefois, dans le cadre d'enquête de pointe et moins spécialisée, le renseignement devrait constituer non seulement un outil d'orientation mais aussi la source de départ de l'enquête comme telle.

De plus, les informations ou le renseignement prennent une valeur différente selon le type d'enquête qui le compose. Par exemple, les unités mixtes pour combattre le crime organisé travaillent sur des thématiques différentes que les unités sur le crime économique. Or, là où il demeure une faiblesse remarquable au plan des enquêtes, c'est la fermeture traditionnelle des unités d'enquête. En effet, il est connu que les membres du crime organisé ont des activités dans plusieurs domaines à la fois. Ils ne segmentent pas leurs approches de la même façon que la police. Un homicide peut être relié à la vente de stupéfiants et aussi à une fraude . Or, les méthodes de la police feront que les interventions seront

ponctuelles et selon la définition qui sera donnée du crime. La création et les interventions des unités mixtes aident à contrevenir à ces approches. Or, la cueillette, la conservation et le partage des informations restent encore totalement tabous et restreints dans le contexte de ces unités. A l'intérieur des unités il existe des frictions quant au partage des informations entre les membres de services différents. A l'extérieur des unités, il existe un mur du silence et du non partage total des renseignements. Les unités mixtes sont certainement une très grande avancée par rapport aux méthodes traditionnelles de la police au pays. Il reste encore de grandes améliorations à apporter afin de les proposer comme modèle. On peut penser que dans un avenir prochain, non seulement des services de police mais également des partenaires des banques, de la police privée de grandes corporations, des agents d'application de la loi reliés à différents ministères, seront appelés à créer de telles unités. Il reste à savoir si la constitution de telles unités de pointe aura comme effet de limiter le partage des informations entre les polices et les partenaires.

En résumé, les conditions de partage sont les suivantes:

1- une philosophie personnelle liée à l'idée que la possession des informations favorise un échange facile entre individus se connaissant;

2- le contexte privilégié des unités mixtes de lutte contre le crime organisé favorise l'accès et l'échange réel des renseignements mais sur une base informelle;

3- A certains moments, lors des procédures d'enquête plus précisément lors de la divulgation de la preuve à l'avocat de la défense;

4- le manque de ressources budgétaires et humaines ferait en sorte que les informations obtenues ne pouvant être gérées par un service de police seraient données à ceux qui peuvent mener à bien une enquête.

3.4- L'alimentation des banques de données - ce qui cause problème

Le partage de renseignements implique nécessairement qu'il y aura eu précédemment une période de cueillette. Cela implique aussi que les renseignements possèdent une valeur par rapport aux besoins de

l'enquête ou des enquêteurs impliqués, ou encore des stratégies de combat. Comme le soulignait un enquêteur: "on est aussi bon que la source que l'on peut trouver" (no 9). En fin de compte, le partage des informations est intimement lié à la cueillette des informations. Nous allons voir que les choses ne sont pas aussi simples et ordonnées dans les pratiques.

Disons d'emblée qu'un des principes de la bonne alimentation des données a été justement décrit par un enquêteur ayant plusieurs années d'expérience : "un enquêteur a besoin de beaucoup d'informations. Si le renseignement ne sert pas dans un dossier mets-le dans la banque, ça peut servir à quelqu'un d'autre" (no 20). Cette remarque montre une attitude ouverte non seulement à la cueillette active des informations mais aussi aux nombreuses possibilités de les partager ultérieurement. Un autre élément concerne la perte des informations. Il semble que les pratiques actuelles des enquêteurs les amènent à focaliser sur les informations très pointues relatives à une enquête. Les informations que l'on dirait secondaires sont laissées de côté : "mon cahier d'enquête est bourré d'informations que je n'ai pas divulguées parce que ça n'intéresse probablement pas personne. Je n'ai pas le temps de tout entrer. Tu fermes ton dossier ça s'arrête là - autrement on en finirait plus de mettre des infos dans les banques"(no 5). Le policier confirme ce qu'un patron d'une grande unité d'enquête avait précédemment constaté : "les gars sont bons pour collecter des renseignements ils ne sont pas bons pour les mettre dans des banques de données" (no 16).

Les pratiques d'alimentation sont affectées par aux moins quatre facteurs. Le premier porte sur le comment faire. Il est significatif qu'un enquêteur ait souligné les manques flagrants au plan d'une méthodologie de travail. Discutant de la cueillette des informations, il dit : "c'est un fardeau d'aller chercher ça. Chaque enquêteur a une information. On a des rapports à faire...alors pour aller chercher les infos on y va à peu près. On regarde ici et là dans des banques etc" (no18). Quant à la transcription des informations dans des banques de renseignements, il est dit une chose étonnante et significative par sa portée. Plusieurs personnes l'ont aussi évoqué dans des termes similaires. "Si je pense que l'information est nécessaire, je vais l'inscrire sinon ça reste dans le dossier" (no 18). L'enquêteur ne donne pas d'explications sur ce qui est nécessaire. Il faut comprendre ici que cela relève du domaine des pratiques et des habitudes traditionnelles d'enquête. Dans le même ordre d'idées, on comprend alors la remarque d'un certain nombre d'enquêteurs à l'effet qu'il n'y a pas le huitième des données qui sont entrées dans la banque qui pourraient être intéressantes....une information pas intéressante pour un enquêteur peut le devenir pour un autre" (no 17). Enfin, encore ici, la charge de travail imposée aux

enquêteurs devient un argument justifiant une alimentation partielle ou encore une non alimentation. "Il faut éviter l'alimentation de plusieurs banques à la fois. Penser qu'un enquêteur va rédiger son rapport, alimenter les banques de renseignements est utopique avec la charge de travail que les enquêteurs ont actuellement" (no 16). Ou encore, "c'est lourd de tout rentrer, il y a les notes personnelles, le rapport à faire, le rapport d'événements et ça n'arrête plus. Il faut faire la synthèse. J'ai pas le temps" (no 22, 18).

Le second facteur s'illustre par les sources d'information. Que va-t-on cueillir? De façon générale, disons que la majorité des enquêteurs rencontrés s'entendraient pour dire que l'information recueillie doit être contemporaine et actuelle parce qu'alors elle est directement utile dans le cours d'une enquête. La cueillette et les efforts déployés pour s'assurer de la pertinence du matériel sont vus comme exigeants et astreignants (no 5, 9). Il semble qu'une fois la collecte terminée, on doit consacrer beaucoup d'efforts pour que soient validées les informations, c'est-à-dire qu'elles ne soient pas seulement des ragots mais du matériel utilisable en enquête (no 20). Ainsi décrit, le processus de collecte n'est pas un encouragement à l'alimentation parce qu'il y a cette idée que l'information est de l'ordre du ragot si elle n'est pas appuyée. Or comme il a déjà été mentionné, un type d'information inutile pour un enquêteur peut s'avérer pertinent pour un autre. De même, plusieurs enquêteurs voient le renseignement comme étant directement utile dans l'enquête au point qu'il pourra être utilisé en preuve au tribunal ou qu'il permettra de procéder à des arrestations et des condamnations : "Le renseignement c'est des outils utilisables en preuve qui permettent de procéder à des arrestations et des condamnations...et sont utilisables pour les opérations" (no 7).

Un troisième facteur porte sur les sources d'information. Il s'agit de voir encore ici s'il existe une dynamique en terme de méthodologie pour tirer le maximum des sources possibles. Telle qu'attendue, la source principale se situe, nous dit-on, dans le champ, ce qui implique de sortir des bureaux et de créer des liens avec des individus, de faire aussi de la surveillance active (no 13). C'est lors de cette période de cueillette qu'il apparaît important que les enquêteurs développent le réflexe de s'intéresser à l'événement dans sa tonalité de sorte que des informations dérisoires finissent par devenir une clé dans la solution. Le patrouilleur est une autre source d'alimentation active. Il est un agent de renseignement dans des cas spécifiques (no16). Grâce à ce qui est nommé le PSU (personne sous surveillance) par la Sûreté du Québec, un patrouilleur qui intercepte un individu le sait immédiatement et agit en conséquence. Il indique la raison de l'interception et indique suivant le cas s'il a besoin d'informations supplémentaires (no 21). Le patrouilleur sert de courroie de transmission car s'il arrive que des

enquêteurs lui donnent des informations, c'est surtout pour aller en chercher qu'on communiquera avec lui (no20).

Un quatrième facteur enfin concerne l'apport de la technologie. On pourrait dire que l'apport de la technologie se mesurerait à l'usage. Or, il apparaît que les ressources techniques nécessaires ne sont pas mises à la disposition des gens. "We do not have the technical ressources to technically service our NCDB. We are not putting enough info into the system" (no 14). Une autre explication repose sur le manque de ressources humaines pour entrer les données dans les banques. On dit : il y a une accumulation des informations mais on n'a pas suffisamment de personnes pour rentrer les données (no 11). Un autre commentaire allant dans le même sens: "on s'est aperçu que ceux qui alimentaient les banques de renseignements étaient ceux qui avaient des personnes dédiées à temps plein pour ne faire que de l'alimentation" (no 16).

En bref, quatre facteurs influencent les pratiques d'alimentation. Ce sont :

1- le "comment faire" qui réfère à une méthodologie de travail ou à son absence;

2- le "quoi colliger" qui rappelle que les pratiques d'alimentation sont beaucoup encouragées dans le cadre d'enquête spécifique et moins pour le bien fondé de créer des banques de renseignements criminels;

3- les sources de l'information directes connues par les techniques traditionnelles, mais aussi l'apport des patrouilleurs;

4- les technologies comme support dans la collecte des informations à la condition qu'elles soient utilisées et qu'elles facilitent le travail de l'enquêteur.

4- La nécessité d'une formation adéquate

La nécessité d'une formation adéquate est nettement reconnue par les interviewés et par beaucoup d'intervenants dans le domaine de la police. Sans aucun doute, la formation adaptée et adéquate favorise un travail de qualité. Certains diront même que la formation se doit d'être spécialisée de sorte

que les policiers puissent suivre rapidement l'évolution de leur domaine d'enquête. La formation en fait devient un des outils de combat de la criminalité dans le sens où "every component is vital to the end result" (no 3). Mais pour cela, il faut qu'elle soit offerte et donnée au moment opportun, ce qui ne semble pas être le cas pour la grande majorité des individus interviewés. Soit que le roulement du personnel est trop rapide, soit que les nouveaux enquêteurs viennent directement de la patrouille et que le temps manque pour leur donner une formation formelle. Enfin, une des grandes difficultés de la formation dans le domaine des enquêtes, mais nous dirions pas exclusivement, est le roulement du personnel. Même si le gestionnaire a planifié un programme de formation général annuel pour les membres de son unité, il reste que le personnel est appelé par le biais des structures de promotion à faire avancer le personnel en allant d'une unité à une autre et selon les disponibilités des concours de promotion. Il arrive donc que le personnel en place ne soit pas formé, ou une fois formé, que les individus soient mutés vers d'autres unités. Tel que mentionné: "le gros du problème est le déplacement du personnel policier. Tu es affecté à un endroit, on te forme et tu vas travailler ailleurs. L'organisation se retrouve dans une situation où elle ne fait que former des gens, des gens avec de la volonté mais sans expérience... La formation ne sert pas parce que les gens se déplacent" (no 17).

Il arrive que l'apprentissage aux fonctions soit fait directement sur le terrain et avec le temps. On dit alors : "ça s'apprend avec le temps" (no 6). La situation n'est guère l'objet de critiques ou de remarques négatives. Les gestionnaires rencontrés espèrent par ailleurs que les enquêteurs finiront par devenir compétents dans l'exercice de leurs fonctions. Ainsi, "avec le rajeunissement, les jeunes proviennent de la route. Ils apprennent avec les collègues. On réussit à avoir des gars compétents" (no 12). L'apprentissage, c'est en d'autres mots : "de demander des conseils aux autres, tu l'apprends en le demandant aux autres" (no 6). C'est aussi : "je l'ai appris à gauche et à droite. Je suis venu à bout d'aller chercher des informations un peu partout" (no22).

Pourtant, un certain nombre ont été en mesure d'évaluer les conséquences résultant d'une absence de formation adéquate ou d'une formation partielle, dite sur le tas, auprès de collègues pas toujours plus expérimentés qu'eux. Par exemple, un enquêteur d'un service de grande taille constatait que 75 p.cent des nouveaux enquêteurs proviennent directement de la patrouille. Ils n'ont aucune expérience dans le domaine des enquêtes, ils n'ont pas d'habiletés, ils n'ont pas d'intérêts, ils ne savent pas comment faire (no3, 4, 9), et ajoutons, ils ont peu de formation pertinente au départ. Il en découle des conséquences immédiates. Elles sont de deux ordres. D'abord les personnes peu ou pas formées doivent

nécessairement se fier aux collègues pour obtenir informations et conseils. Cela veut dire une perte de temps appréciable autant pour les nouveaux venus que pour les policiers d'expérience. Il s'agit donc pour l'individu concerné, de s'assurer de se créer un réseau de contact qui lui fournit les informations pertinentes ou encore de trouver des personnes-ressources adéquates. "Si on est pas capable on va voir d'autres personnes qui connaissent ça....ça le retarde et ça nous retarde" (no 18). Et aussi, "si je suis pas en mesure de l'enquêter...je vais aller chercher une personne ressource pour chercher les indices...je lui demande des références ou des choses spécifiques" (no 22). Par ailleurs la nécessité de s'en remettre constamment, du moins pour un temps indéfini, aux collègues signifie potentiellement des erreurs ou l'absence d'action. "Il est laissé à lui-même, il se débrouille. C'est pas facile. Des fois il part trop à droite ou à gauche. Il tourne en rond parce qu'il ne sait pas où il va.....j'ai vu souvent des gens interpréter à tort et à travers et dire des faussetés" (no 23). Il peut arriver aussi des conséquences plus dramatiques où des erreurs judiciaires entraînent la perte de causes qui ont engendré des coûts élevés : "...when police officers are making mistake it is a huge backward case law...we are losing tax payers money.."(no 2).

Nous avons demandé aux individus s'il y avait des thèmes ou des questions plus spécifiques qui devraient être traités lors des programmes de formation. Pour l'un deux, il n'est pas évident qu'il faille développer des programmes de formation mais plutôt d'offrir davantage une formation de pointe et à la carte. De la sorte, les besoins spécifiques d'une clientèle type peuvent être rencontrés en particulier dans le domaine des technologies de l'information. "Au niveau technologique, le problème est l'évolution des technologies. Je ne connais pas une école qui peut suivre...on a orienté notre formation sur-mesure. On veut amener nos gens à une base standard" (no 19). On a dit aussi qu'il est important d'encourager les individus à se tenir au courant des développements dans leur domaine d'expertise. Nommée "formation indirecte", elle permet aux individus "d'être éveillés, de se tenir au courant de l'environnement, de connaître les tendances...etc" (no 19).

La formation concerne aussi et surtout le développement des législations et de la jurisprudence. L'une comme l'autre exercent une influence sur les pratiques et sur les façons de travailler. Comme le constatait un gestionnaire, "il faut être au courant de ça" (no 9, 2). La formation concerne aussi les habiletés et les techniques d'application de la loi, les pratiques avec les informateurs, l'usage adéquat des banques de données, les techniques d'infiltration de groupes organisés, les langues d'usage, etc (no 4, 9, 2, 3).

La formation dans le domaine des enquêtes, entre autres celle sur le crime organisé et la cyber-criminalité, n'a pas été reçue systématiquement par les policiers interviewés quel que soit le service de police auquel ils appartiennent. Plus souvent qu'autrement, la formation est donnée sur le tas à partir des contacts et des demandes faites entre collègues, les plus expérimentés enseignant aux plus jeunes. Les programmes de formation portant sur les niveaux d'enquête, débutant et avancé, sont vus comme pertinents de la part de ceux qui les ont suivis, soit très peu de personnes interviewées. Par contre, il y a un consensus sur la nécessité de maintenir à jour les enquêteurs par rapport à l'évolution des législations, de la jurisprudence et des habiletés développées. Car, a-t-on dit, ils influencent directement les pratiques des enquêteurs et les résultats obtenus. Dans le domaine des technologies, on est d'avis que les formations sur mesure répondent davantage aux besoins des policiers impliqués.

Il a aussi été mentionné que trop souvent les budgets font l'objet de coupures budgétaires. Mesures efficaces sur le coup pour les gestionnaires de la police, il ressort qu'à long terme, les pratiques policières s'en ressentent définitivement soit par des bavures, des erreurs judiciaires ou tout simplement des façons inadéquates d'enquêter.

Dans un monde idéal, tous les crimes rapportés seraient enquêtés et un certain nombre d'entre eux solutionnés par des professionnels de l'enquête et du renseignement. Or, dans les faits, il n'est pas rare qu'une plainte d'un citoyen ne soit pas retenue par manque de temps, de budget ou tout simplement de compréhension des complexités de la plainte. Certaines des plaintes retenues feront l'objet d'une enquête, quelquefois approfondies et quelquefois non. On pourrait dire que les résultats dépendent en grande partie des compétences des policiers et de leur professionnalisme pour recevoir, pour enquêter et pour apporter des solutions acceptables. Dans un environnement en grand bouleversement, il devient d'autant plus important de fournir aux enquêteurs une formation adaptée à cet environnement.

En bref, il apparaît que la formation dans le domaine des enquêtes et des enquêtes reliées aux crimes technologiques n'est pas suffisante. Il semblerait selon les interviewés qu'il n'y a eu suffisamment de formation reçue.

Par ailleurs, les programmes de formation ne sembleraient pas suffisamment adaptés à la nouvelle réalité à laquelle les enquêteurs sont confrontés. La société évolue à un rythme plus rapide que la police.

De plus, les programmes de formation sont mis à jour sans suivre la cadence de l'évolution du marché des technologies. S'il est vrai qu'un enquêteur doit apprendre avant tout à enquêter avant d'apprendre à enquêter un crime informatique, il reste que des ajustements sont nécessaires face aux nouveaux outils technologiques qui permettent des actions révolutionnaires et complètements nouvelles.

4.1- Des conditions essentielles de succès à créer

On a vu à partir des représentations des interviewés qu'il existe une dynamique complexe et intéressante dans le champ des enquêtes criminelles, en particulier celle relative au crime organisé et au cybercrime. On a constaté qu'il y a souvent un décalage entre ce que les gens disent qu'ils font dans leur pratique quotidienne et ce qu'ils font réellement à cause de leur compétence, de leurs habiletés, de leur formation passée, de leur intérêt personnel et des budgets disponibles. Nous avons aussi examiné les initiatives qui facilitent des interventions communes de différents services de police à défaut d'encourager la cueillette et le partage des informations et du renseignement criminel. Nous avons commenté ailleurs les éléments qui devraient être inclus dans un programme de formation pour les enquêteurs, en particulier pour les crimes émergents. Il reste à notre avis un dernier point à examiner. Il porte sur les facteurs de succès de la police dans le combat contre la criminalité. S'il est vrai que la littérature est abondante sur les programmes de formation pour les recru(e)s et pour la formation continue, elle est moins abondante par contre sur ce qui fait qu'un programme de formation atteint ou non ses objectifs. Nous ne parlons pas ici des objectifs relatifs au contenu d'un cours, mais des objectifs plus larges relatifs à l'usage des contenus donnés mais aussi et surtout au rapport que les individus entretiennent avec ces contenus. Pour le dire autrement, si les individus ne croient pas dans ce qui leur a été enseigné, ou qu'ils ne peuvent pas appliquer ce qui leur a été donné, il en résulte que le champ de pratique ne peut être amélioré.

Plusieurs facteurs déterminant la bonne marche d'une enquête peuvent être identifiés. Il faut un personnel en nombre suffisant, des budgets adéquats, une formation donnée et adaptée, l'usage d'outils technologiques de pointe, etc. Un programme de formation n'exerce aucune influence sur la plupart de ces facteurs. Il peut potentiellement jouer par contre sur les attitudes et sur les mentalités. Il peut aussi améliorer les compétences des individus. Mais pour ce faire, il reste des ponts à franchir.

Dans son livre sur les techniques d'enquête sur les ordinateurs, Mendell (1998) s'intéresse à

l'environnement global des technologies de l'information. Il fait un commentaire extrêmement déterminant sur le succès futur d'une formation et des enquêtes quand il dit : "...intelligence seeks to perceive what is not immediately apparent. By integrating both rational facts and intuitive insights, intelligence offers a holistic picture" (p.53). Le vrai défi pour l'enquêteur, et ajoutons ici l'analyste, est de dépouiller les faits en faisant appel à la fois au bon jugement, à l'intuition et à la déduction. Ces aspects deviennent d'autant plus importants que les technologies de l'information ont engendré de nouvelles façons de communiquer, un langage, des façons de faire ainsi que leurs propres épiphénomènes nommés *hacker, cracker, phreaker*. On parle désormais de la culture des *hackers* (Taylor, 1999) et bien d'autres. Il semblerait aussi qu'il existerait déjà un conflit de génération parmi les *hackers*, les plus jeunes ayant grandi avec l'usage régulier de l'ordinateur à la maison. Or, les programmes de formation offerts aux policiers mettent probablement trop de côté les qualités à développer parce que cela implique un investissement personnel important à plus ou moins long terme et qui demande une certaine distance par rapport aux techniques magiques enseignées. Ces qualités semblent se situer en conjonction directe avec la culture des technologies de l'information. Ce n'est pas seulement le langage des ordinateurs qu'il faut posséder mais aussi la compréhension du nouvel environnement qu'il crée.

Dans un univers en développement aussi rapide, les futurs enquêteurs devraient avoir les compétences suivantes: expérience, compétence, bonne capacité d'analyse, souplesse pour adapter son milieu de travail à l'évolution des technologies, aux législations à venir et à leur application. Il serait aussi souhaitable que les individus puissent créer un système de réseau avec l'entreprise privée des technologies (voir entre autres Meyer, Short, 1998).

A la suite de Mendell, nous dirions que la formation devrait porter non seulement sur les techniques, ce qui est déjà couvert, mais également sur des exercices de logique, de déduction et d'évaluation des cas difficiles. Des exercices sous forme de scénarios devraient favoriser l'*input* des étudiants, leur capacité de compréhension et de développement et leur faculté de déduction. Comme l'ont très justement souligné Boni et Kovacich (1999:36), un des plus importants défis pour l'application de la loi et la sécurité moderne consiste à apprendre à penser et à opérer dans un nouvel environnement dynamique créé par les technologies.

Par ailleurs, d'autres pistes demandent à être explorées. Elles concernent les entreprises de

collaboration entre la police et divers groupes intéressés par la sécurité. Elles portent aussi sur les alliances entre les différentes agences gouvernementales et aussi entre les pays. Le but ultime est de prévenir le crime, entre autres, le crime organisé et le crime sur le *net*. La vraie question est comment parvenir à actualiser les partenariats? Chaque organisation est soumise à des normes légales, à des champs de pratique et à des règles éthiques. De plus, dans un contexte où les pressions des élus sur la police pour qu'elle repense ses approches de service aux citoyens, qu'elle donne priorité aux victimes de crime et contrôle ses coûts d'exploitation, les crimes sans victime deviennent moins prioritaires. Ce type de crime est très exigeant au plan des ressources humaines et budgétaires (filature, support aux opérations, écoute électronique, surveillance physique). Il arrive comme souligné que "la réalité ce sont des corporations qui enregistrent des pertes importantes perçues par les autorités locales comme des crimes sans victime. Il y a un danger présentement que les municipaux disent ont va prendre ton enquête mais comme je n'ai pas de ressources autres que des enquêteurs ça va prendre de l'argent pour payer des délateurs, pour défrayer mon support aux opérations....ca se fait beaucoup maintenant..."(no 31).

Quels sont les enjeux en présence, quelles sont les possibilités de partage des informations possédées par les unes et les autres, quels sont les outils disponibles pour le faire, quelles sont les limites au partage des renseignements personnels possédés à la lumière des lois sur la vie privée, quelles sont les embûches techniques à surmonter, tels sont les points majeurs à évaluer afin de parvenir à créer des partenariats dans le combat contre le crime. Il y a aussi le fait que l'industrie est prête à collaborer avec la sécurité publique jusque dans une certaine limite. L'industrie ne veut pas en général mettre en péril son rapport privilégié avec ses clients, les citoyens

On peut imaginer qu'une mise en commun des outils, des méthodes de travail et des intérêts communs pourrait se faire lors de séminaires de formation pointue et adaptée à la réalité des organisations en présence. Ils pourraient probablement aussi être structurés dans un contexte de formation en ligne ou à distance (Mulholland, 2000).

Le partenariat s'illustre aussi par le biais d'une certaine forme de coordination entre les agences d'application de la loi. On peut imaginer le développement d'une banque de données qui porterait par exemple sur les formes sophistiquées de crimes technologiques, sur les modèles d'action, pour développer par la suite des programmes de prévention. On peut voir aussi le développement d'une liste d'acteurs ou d'unités dans le domaine de l'application de la loi qui se penchent particulièrement sur le

crime organisé et sur le *cybercrime*. Des enquêtes faites par des firmes spécialisées sur l'état de la pénétration des systèmes informatiques pourraient être d'une grande utilisé pour les processus de prise de décision dans la police.

Une approche pragmatique mérite d'être mentionnée ici. Aux États-Unis, le ministère de la Justice (U.S.A. Department of Justice, 2000) a développé une page Internet d'informations spécialement adaptées aux enfants sur ce qu'Internet permet de faire et ce qui ne doit pas y être fait. Le même type de page a aussi été développé pour les citoyens en général pour les conscientiser comme citoyens et comme parents face à l'univers Internet en développement. La logique est simple. Comme la technologie permet un accès direct et immédiat à des sources d'information de tout genre et de toute provenance, on doit enseigner à tous les individus à développer une éthique d'usage de l'Internet, éthique on le comprend qui gagne à être développée le plus tôt possible en bas âge. Une autre approche récente a été la création d'un laboratoire scientifique d'ordinateurs dans la région de San Diego qui fait appel à un partenariat entre les agences d'application de la loi au niveau local, fédéral et des états. En mettant ensemble les ressources disponibles, les agences augmentent substantiellement leur potentiel (Robinson, 2000).

Conclusion

Ce rapport a cherché à diagnostiquer la question de la collecte des informations, de l'alimentation des banques de données et du partage des informations entre les collègues et entre services de police. Nous avons particulièrement focalisé notre attention sur le crime organisé et sur les crimes cybernétiques, deux champs complexes et en pleine émergence. Nous avons voulu examiner comment les policiers, les analystes de la criminalité et les décideurs voyaient les façons de faire dans les enquêtes et quels types de solution ils prévoyaient y apporter. Ce dernier aspect reste particulièrement peu étoffé.

Nous pensons qu'une fois les obstacles identifiés et nommés ainsi que les facteurs de succès actuels il deviendrait possible de favoriser l'échange des renseignements, d'améliorer la performance des individus et peut-être aussi de créer des standards nationaux au plan de la cueillette des informations, des niveaux de sécurité à établir et des approches pour favoriser la confiance entre les partenaires.

Il ressort que les limites actuelles dans le domaine des enquêtes se résument ainsi. Il y a un personnel insuffisant et en continuel mouvement. Il arrive que des individus de l'unité des homicides soient prêtés à une autre unité, ou encore que les équipes qui se penchent sur le crime informatique soient petites. Il arrive aussi très régulièrement que les individus quittent une unité d'enquêtes pour avoir droit à une promotion. Ils quittent alors avec une expertise pour aller en développer une autre ailleurs. En outre, plusieurs des interviewés ont commenté le fait que les budgets disponibles étaient trop souvent limités, ou que leurs budgets actuels ne leur permettaient pas d'avoir accès aux outils nécessaires pour mener des enquêtes efficaces.

En ce qui concerne la formation des enquêteurs, on pourrait dire qu'elle n'est pas toujours adaptée au contexte, qu'elle n'est pas offerte au bon moment, encore qu'elle n'a jamais été reçue et enfin qu'elle est vue comme essentielle. Dans le cadre d'un programme de formation, il va se soi que les législations et la jurisprudence doivent être connues. Il va se soi également qu'elles demeurent un des piliers relatifs aux enquêtes. Il est donc essentiel de connaître les subtilités de la partie VI du Code criminel en ce qui concerne les affidavits. D'autres aspects de la formation concernent les habiletés à développer pour travailler avec des collègues de son service de police, d'autres services de police ou d'autres agences d'application de la loi.

Il ressort que par rapport aux crimes reliés aux technologies de l'information, il faut développer une expertise d'enquête au plan de la compréhension des façons de faire plutôt que d'essayer de devenir un expert en informatique ou en gestion de système. Il existe une grande catégorie d'experts dans le domaine des technologies. Il reste donc aux policiers à apprendre à travailler avec ceux-ci.

Le domaine de la sécurité publique est confronté à plusieurs types de banques de données. Certaines sont nationales comme le Centre d'information de la police canadienne, d'autres appartiennent à un service de police, comme la BNDC de la GRC, ou relèvent d'un organisme comme l'Agence canadienne des douanes et du revenu, etc. De plus, l'accessibilité à une banque est aussi compliquée. Il existe divers niveaux de sécurité pour les membres d'un service de police et également pour les autres services de police. En plus, il y a le grave problème de l'incompatibilité des systèmes informatiques. A cela s'ajoute la problématique de l'alimentation des banques en vertu de la confiance que les individus y portent et aussi du temps disponible pour entrer leurs données. Enfin, il demeure une question très peu touchée à l'égard des informations, à savoir la qualité du matériel colligé. S'il est vrai que les

informations devraient aider une prise de décision éclairée pour une enquête, il reste que la pertinence des informations est trop peu soulignée. Ainsi, une fois que les policiers ont dépassé la barrière du droit de savoir et du besoin de savoir, il reste des écueils au plan de la transparence entre collègues, de la confiance mutuelle à créer et des possibilités physiques de partager les informations.

En ce qui touche le *cybercrime*, le terrorisme informatique et les nouvelles formes de crime reliées à l'environnement, on peut dire sans se méprendre qu'il y a à ce jour une méconnaissance réelle des problématiques et des enjeux. Plus souvent qu'autrement, les interviewés ont vu ces questions comme relevant d'unités spécialisées ou encore d'agences autres que la police. En ce sens, on peut dire que la police prépare peu ses policiers à l'évolution de la société.

Enfin, dernier commentaire, il existe définitivement une culture des enquêtes. Cette culture maintient les individus dans des boîtes que certaines nomment silos, qui contrevient d'une certaine façon à la collaboration entre collègues, au partage des informations et finalement au succès des enquêtes. Une piste de solution serait de former les enquêteurs dans des programmes de formation conjoints sur la collaboration, sur le partage et aussi sur la capacité d'aller chercher l'expertise là où elle se trouve. Encore maintenant, le partage se fait d'une façon unilatérale de la part de la police avec les agences et entre services de police de grande taille avec ceux de moindre taille, et avec les grandes corporations qui collaborent avec la police, ce qui devient contre-productif à moyen terme et long terme. Il reste donc à développer une culture du renseignement qui ne soit pas limitative.

Une approche proposée vise à focaliser sur les types de partenariat à créer avec les autres agences d'application de loi dans l'esprit des meilleures pratiques et des grandes leçons retenues. Elle pourrait également être orientée sur le type de partenariat à développer avec la police privé, les agences de sécurité des grandes corporations comme les banques, par exemple. Enfin, on pourrait également focaliser sur le partenariat à développer avec la grande industrie reliée aux technologies de l'information. Ces dernières assument la responsabilité de développer des outils pour la société. Il appartient à la police de développer des approches qui permettraient d'utiliser efficacement ces outils.

Références

Alexander, K.; Munro, R. (1996). Cyberpayments: Internet and Electronic Money Laundering: Countdown to the Year 2000. *Journal of Financial Crime*, 4, 2:156-160.

Benson, D. (1993). The Police and Information Technology. In G. Button (ed.) *Technology in Working Order*. London: Routledge.

Blackburn, W. (2000). Credit Card and Debit Card Fraud in the Year 2000. *The Report on Crime & Profiteering*, 4,1:6.

Boni, W; Kovacich, G. (1999). *I-Way Robbery. Crime on the Internet*. Boston: Butterworth Heinemann.

Canada, Department of Justice. (2000). Electronic Commerce. Http://Canada.justice.gc.ca Consulté le 00/09/15

Carter, D.; Katz, A. (1998). Computer Applications by International Organized Crime Groups. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas

CSIS Global Organized Crime Project. (1998). *Cybercrime, Cyberterrorism, Cyberwarfare. Averting an Electronic Waterloo*. Washington: CSIS.

Davis, R.; Hutchison, S. (1997). *Computer Crime in Canada*. Toronto: Carswell.

Deloitte Touche Tohmatsu (1999). Cracking Computer Fraud: A U.S. View. *The Report on Crime & Profiteering*, 3, 1:6-7.

Denning, P.J. (1998). The Internet after Thirty Years. In Denning D.; Denning, P. (ed.). *Internet Besieged. Countering Cyberspace Scofflaws*. New York: ACM Press.

Dertouzos,J; Larson, E. ; Ebener, P. (1999). *The Economic Costs and Implications of High-Technology Hardware Theft*. USA. CA, Santa Monica: Rand. Science and Technology Program.

Drolet, J.F.; I. Moen (2000). Enabling the Next Generation of Defence Capability. Nanotechnology. *Vanguard*, 6:22.

Dryden, J. (1998). La montée en puissance du commerce électronique. L'Observateur, no 214,

octobre-novembre, www.oecd.org//publications/observer consulté le 1999-20-10.

Ekos Research Associates Inc. (2000). The Public Opinion Environment and Emerging Trends in Public Security. Presentation to SEC/Co /Directors Planning POWPM. March 28.

Federal Bureau of Investigation, (1999). Encryption: Impact on Law Enforcement. Www.fbi.gov/library/encrypt/encryppt.htm consulté le 12/04/00.

Field, M. (2000). Organizational Dynamics in a Technology-Driven World; The Impact of Email on Law Enforcement, *The Police Chief*, February, 45-49.

Gendarmerie Royale du Canada (2000). Environnement de la GRC. Tendances. www.infoweb.a.rcmp-grc.gc.ca

Hamilton, H. (2000). The Effective Use of Partnerships to Reduce the Impact of Organized Crime: How Ontario' CFSEU Balances the Responsibility. *The Gazette*, 62,3: 17-23.

IACP (1999) Best Practices for Seizing Electronic Evidence, www.theiacp.org consulté le 12/04/00

Icove, D.; Seger, K. ;VonStorch, W. (1995). *Computer Crime. A Crimefighter's Handbook*. Sebastopopl, CA: O'Reilly & Associates, Inc.

LeBeuf, Marcel-Eugène (2000a) *La police et l'usage des technologies de l'information: un bilan actuel*. Ottawa: Écoles des sciences policières, Collège canadien de police. Disponible à: www.cpc.gc.ca

LeBeuf, M.E. (Ed.) (2000b) Police and Information Technology: Understanding, Sharing and Succeeding, May 28-30, 2000. *Conference Proceedings*, September. Ottawa: Canadian Police College (CD-ROM.).

LeBeuf, M.E. (2000c). *Les implications de l'usage des technologies de l'information pour les enquêteurs dans la police au Canada*. Ottawa: Ecole des sciences policières, Collège canadien de police. Disponible à www.cpc.gc.ca

LeBeuf, Marcel-Eugène, Paré, Simon; Belzile Miguel (1999). *Les technologies de l'information dans la police au Canada: portrait actuel*. Écoles des sciences policières, Collège canadien de police.Disponible à: www.cpc.gc.ca

Lenton, W. (2000). Official Welcome. Pacific Rim Money Laundering & Financial Crimes Conference, Vancouver, October 20-24.

Livanos Cattaui, M. (1999). Alliance Against Commercial Cybercrime. Conference Report.International Chamber of Commerce. London, 7 December. Http://www.iccwbo.org/home/conferences/reports Consulté le 00/20/10

Mendell, R. (1998). *Investigating Computer Crime. A primer for Security Managers*. Springfield: Charles C. Thomas Publisher Ltd.

Meyer, J.; C. Short (1998). Investigating Computer Crime. Police Chief, www.theiacp.org consulté le 00/12/ 4

Mulholland, David (2000), Technology Training and Education Opportunities, Police Chief, 03/03/2000, www.theiacp.org consulté le 12/04/00

Murray, A.D.; Vick, D.W.; Wortley, S. (1999). Regulating E-commerce: Formal Transactions in the Digital Age. *International Review of Law Computers & Technology*, 13,2:127-145.

Nations Unies, Rapport du Secrétaire général (1999). Situation de la criminalité et de la justice pénale dans le monde. *Dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants*. Vienne, 10-17 avril 2000.

Norman, D. (2000). The State of On Line Learning. *Training*, September.

Organized Crime Digest (2000a). Teens Arrested for Cyber Fraud. (January) 21,2:3.

Organized Crime Digest (2000b). Internet Thefts Create New Risks. (Marsh) 21,5:5.

Organized Crime Digest (2000c). 29 Nations Will Work for Uniform Policies Against Cyberfraud. (August), 21,16:3.

Osterburg, J. W.; Ward, R. (1997). *Criminal Investigation: A Method for Reconstructing the Past*. 2nd ed. Cincinnati: Anderson Publishing Company.

Parsons, M. (1998). Crime Orevention and the Electronic Frontier, FBI Law Enforcement Bulletin, www.fbi.org consulté le 12/04/00

Porteous, S. (2000). The Greening of Intelligence. *Crime & Profiteering*, 4, 3:13-14.

Porteous, S. (1998). *Organized Crime Impact Study. Highlights*. Ottawa: Public Works and Government Services of Canada.

Richards, J. (1999). *Transnational Criminal Organizations, Cybercrime, & Money Laundering: Handbook for Law Enforcement Officers, Auditors, and Financial Investigators*. Boca Raton:

CRC Press.

Robertson, J. (1999). The Changing Face of White -Collar Crime, *Police Chief*, www.theiacp.org consulté le 12/04/00

Robinson, M. (2000). Law Enforcement Response to Cyber-Crime. Police Chief, www.theiacp.org consulté le 12/04/00

Sambugaro, E. (2000). Cyberspace and the Criminal E-economy. *The Report on Crime & Profiteering*, 3,4:4-5.

Sambugaro, E. (1999). Cybercash Aids Organized Crime Money Launderers. *The Report on Crime & Profiteering*, 3,3:7.

Scientific American (2000). Internet_Anonymity. Speech without Accountability. Octobrer:34.

Sheriff (1999), Computer ans Internet Crimes, www.theiacp.org consulté le 12/04/00

Smith, R. (1999). Defrauding Governments in the Twenty-first Century. *Trends & Issues in Crime and Criminal Justice*, no.111. Australian Institute of Criminology.

Soullière, Nicole (1999). *Police et technologies: un bilan historique, un regard contemporain.* Ottawa: Écoles des sciences policières, Collège canadien de police. Disponible à: www.cpc.gc.ca

Sullivan, S. (1999), Policing the Internet, FBI Law Enforcement Bulletin, www.fbi.gov consulté le 12/04/00.

Taylor, P. (1999). *Hackers. Crime in the digital sublime*. London: Routledge.

TELEMASP Bulletin (2000). An overview of computer-related crime. *TELEMASP Bulletin*,7,1:1-11.

The Report on Crime & Profiteering (2000). "GetRichQuick.com": FTC Sweeps the Internet for Scammers. 4,1:9.

Thompson, E.P. (1975). *Whigs and Hunters. The Origin of the Balck Act*. New York: Pantheon Books.

U.S.A. Department of Justice (2000), Cyber Ethics, www.cybercrime.gov consulté; le 00-10-20

U.S.A. Government (1999) Cyberstalking: A New Challenge for Law Enforcement and Industry. A Report from the Attorney General to the Vice-President. www.theiacp.org consulté le 12/04/00

Wall, D.S. (1998). Catching Cybercriminals: Policing the Internet. *International Review of Law Computers & Technology*, 12, 2:201-218.

White, L. (2000). Ernst & Young Survey Finds a New Generation of Fraudsters. *The Report on Crime & Profiteering, 4,2:7.*

White, C. (2000). Egg Bank Robbery: Cyber-bandits on a Roll? *The Report on Crime & Profiteering,* 4,3:17.

Williams, W. (1999). The National Cybercrime Training Partnership. *The Police Chief,* February: 17-27.